GROUPS OF ORDER p^3q^2

BY

MYRON OWEN TRIPP

SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, IN THE FACULTY OF PURE SCIENCE, COLUMBIA UNIVERSITY

PRESS OF
THE NEW ERA PRINTING COMPANY
LANCASTER, PA.
1909

GROUPS OF ORDER p^3q^2

BY

MYRON OWEN TRIPP

I.

Introduction.

1.* *Historical note.* Cayley † called attention to an important desideratum in the theory of groups, viz., the determination of all groups of a given order n; for $n = 2, 3, 4, 5, 6$ he found all the types of G_n. A. B. Kempe ‡ enumerated the types of $G_n (n = 1, 2, \cdots, 12)$ and gave a graphical representation in each case. Cayley § remarked that in studying types of groups up to order 11 the first case that involves difficulty is G_8. He also called attention to the fact that Kempe (l. c.) made an error in enumerating the types of G_{12}. Cayley and Kempe proceeded according to order, e. g., they treated G_6, but did not deal with G_{pq} in general. Burnside ‖ gives the number of distinct types for all orders less than 32. The determination of the number of types of G_{32} caused considerable discussion. Concerning these types Levavasseur ¶ said, "I have already found more than 75 distinct groups, and I have not yet finished the enumeration." Shortly afterwards Miller announced ** that the number of these groups is 51. About two years later Bagnera †† stated that the number of G_{32} is only 50. Since then, however, he has conceded that Miller was correct in saying the number of these groups is 51.

All G_p are cyclic. The types of G_{p^2} and G_{pq} are given by Netto.‡‡ G_{pqr}, G_{p^2q} and G_{p^3} have been discussed by Cole and Glover, §§ while G_{p^3} and G_{p^4} have been treated by Young.‖‖ A very important memoir is that of Hölder ¶¶ on

* Throughout this paper the letters $p, q, r, \cdots$, denote different prime numbers. A group of order $p^\alpha q^\beta \cdots$ is denoted by $G_{p^\alpha q^\beta} \cdots$, while subgroups are denoted by H's with subscripts to indicate their orders.

† American Journal of Mathematics (1878), vol. 1, pp. 50–52.

‡ Philosophical Transactions (1886), vol. 177, pp. 1–70.

§ American Journal of Mathematics (1888), vol. 2, pp. 139–157.

‖ *Theory of Groups*, p. 105 and chap. V.

¶ Comptes Rendus (1896), vol. 122, p. 182.

** Comptes Rendus (1896), vol. 122, p. 370.

†† Annali di Matematica (1898), p. 139.

‡‡ *Substitution Groups*, Cole's Translation, p. 149.

§§ American Journal of Mathematics (1893), vol. 15, pp. 191–220.

‖‖ American Journal of Mathematics (1893), vol. 15, pp. 124–178.

¶¶ Mathematische Annalen (1893), vol. 43, pp. 301–412.

groups of orders p^3, pq^2, pqr, p^4. The others who have dealt with groups, whose orders are represented by four primes, are WESTERN * on G_{p^3q}, LEVAVASSEUR † on $G_{p^2q^2}$, HÖLDER ‡ on $G_{pqrs\ldots}$, GLENN § on G_{p^2qr}, and MILLER ‖ ¶ on G_{8p} and G_{2p^3}.

The following have enumerated the types of groups whose orders are represented by five primes: BAGNERA ** on G_{p^5}; LEVAVASSEUR †† on G_{16p} (p odd).

Recently POTRON has given a list of the types of G_{p^6} in his Paris thesis.

As regards the solubility of $G_{p^\alpha q^\beta}$, it may be noted that this was proven by SYLOW ‡‡ for $\beta = 0$, by FROBENIUS §§ for $\beta = 1$, by JORDAN ‖‖ for $\beta = 2$, by COLE ¶¶ for $\beta = 3$, by BURNSIDE *** for all values of β.

Objects and results of the present investigation. The principal aim of this discussion is the determination of the defining relations for all distinct types of abstract $G_{p^3q^2}$, no one of which is simply isomorphic with any other. As the number of primes, either the same or different, increases the problem complicates with remarkable rapidity. This is seen on comparing Hölder's treatment of G_{pq} with that of G_{p^2q}. One of the most important parts of the process of obtaining types is the determination of the invariant subgroups necessary for defining the types, which frequently involves considerable difficulty. When one of the primes p or q is 2 the determination of the defining relations becomes more difficult, in general, than for larger values. This arises from the fact that the invariant subgroups which exist for a prime greater than 2 do not necessarily exist when p equals 2.

The number of H_{p^3} and H_{q^2} is given for every type of $G_{p^3q^2}$. Especial attention is also given to decomposable groups, that is, those $G_{p^3q^2}$ which can be formed by taking the direct product of two or more subgroups of lower order. Thus the defining relations of the decomposable groups may be checked by comparing with results previously worked out. The non-decomposable groups are checked by using all possible relations to discover if any inconsistency arises. In many cases, dependent on certain relations between p and q, the number of different types increases indefinitely as p or q increases. This is not the case with groups of orders, p, p^2, pq, p^3 or p^4; but it is the case with

* Proceedings of the London Mathematical Society (1899), vol. 30, pp. 209–263.

† Annales Scientifiques de l'École Normale Supérieure (1902), pp. 335–353.

‡ Göttinger Nachrichten (1895), pp. 211–229.

§ Transactions of the American Mathematical Society (1906), pp. 137–151.

‖ Philosophical Magazine (1896), vol. 42, pp. 195–200.

¶ Quarterly Journal of Mathematics (1898), pp. 259–263.

** Annali di Matematica (1898), pp. 137–228.

†† Annales Toulouse (1903), pp. 63–123.

‡‡ Mathematische Annalen, vol. 5, p. 588.

§§ Berliner Sitzungsberichte (1895), p. 185.

‖‖ Liouville's Journal (1895), vol. 4, p. 21.

¶¶ Transactions of the American Mathematical Society (1904), pp. 214–219.

*** Proceedings of the London Mathematical Society (1904), p. 392.

groups of orders p^2q, p^3q, and p^2q^2. In a few cases the existence of the $G_{p^3q^2}$ requires that one of the primes shall be of a certain form. In § 4 (ii) the existence of one $G_{p^3q^2}$ requires that $q = 8n + 3$, while the existence of another type requires that $q = 8n + 7$. No similar case, in other writings, has come under my notice.

2. *Discussion of those $G_{p^3q^2}$ having neither an invariant H_{p^3} nor an invariant H_{q^2}.* From Sylow's theorem we know that if r^a is the highest power of a prime r which divides the order of a group, the group contains a H_{r^a}. Hence our $G_{p^3q^2}$ must contain one or more H_{p^3} and, also, one or more H_{q^2}.

(i) $p > q$. We cannot have qH_{p^3}, for this requires that $q \equiv 1 \pmod p$ and hence $q > p$. If there are $q^2H_{p^3}$, then $q^2 \equiv 1 \pmod p$ and since we suppose $p > q$ we must have

$$q \equiv -1 \pmod p.$$

Hence we must have $p = 3$, $q = 2$.

(ii) $p < q$. We cannot have pH_{q^2}, for then we would have the congruence

$$p \equiv 1 \pmod q$$

and therefore $p > q$. If there are $p^2H_{q^2}$, then we must have the congruence

$$p^2 \equiv 1 \pmod q$$

which, in view of the hypothesis that $p < q$, gives

$$p \equiv -1 \pmod q.$$

Hence $$p = 2, \qquad q = 3.$$

If there are $p^3H_{q^2}$, either

$$p \equiv 1 \pmod q \qquad \text{or} \qquad p^2 + p + 1 \equiv 0 \pmod q.$$

The former congruence is impossible, for we suppose $p < q$. Since we are considering the case of q or $q^2H_{p^3}$, we must have

$$q = kp - 1 \qquad \text{or} \qquad q = kp + 1 \quad (k = \text{a positive integer}).$$

(*a*) $$q = kp - 1.$$

We must now have the relations

$$p^2 + p + 1 = lq \qquad (l = \text{a positive integer}).$$

$$q + 1 = kp.$$

Since $q > p$ and $q \equiv -1 \pmod p$ we must have

$$l < p \text{ and } l \equiv -1 \pmod p$$

and, therefore, $$l = p - 1.$$

Hence $$p^2+p+1\equiv 0\,[\mathrm{mod}\,(p-1)].$$

If $p \neq 2$, then $p-1$ is always even and p^2+p+1 is odd. Hence we must have $p=2$ and therefore $q=7$

(*b*) $$q = kp+1.$$

We also have $$p^2+p+1=lq.$$

Since $q>p$ and $q\equiv 1 \pmod p$, $l=1$, so that

$$p^2+p+1=q.$$

The only possibilities then that a $G_{p^3q^2}$ may have neither an invariant H_{q^2} nor an invariant H_{p^3}, are for the orders 72, 108, 392 *or for the case in which*

$$p^2+p+1=q.$$

Now in (*b*) where $p^2+p+1=q$, two of the $p^3H_{q^2}$ have an H_q in common which is invariant in the $G_{p^3q^2}$. We thus get a factor group Γ_{p^3q} with p^3H_q and hence only one H_{p^3}. Therefore, our $G_{p^3q^2}$ has an invariant H_{p^3q}. If now this H_{p^3q} had an invariant H_{p^3}, it would be invariant in the whole $G_{p^3q^2}$. Hence the H_{p^3q} must have qH_{p^3}. Now $q-1=p^2+p$ and, since p^2+p is not divisible by p^2, two H_{p^3} have in common an H_{p^2}, invariant in the H_{p^3q} and common to all the H_{p^3}, and hence invariant in our $G_{p^3q^2}$. We thus get a factor group Γ_{pq^2} with an invariant H_{q^2}, since $p<q$. Hence $G_{p^3q^2}$ has an invariant $H_{p^2q^2}$. The latter has an invariant H_{q^2} and hence this H_{q^2} is invariant in our $G_{p^3q^2}$. We can now state the important result, viz.: *With the possible exceptions of G_{72}, G_{108}, G_{392}, all $G_{p^3q^2}$ contain either an invariant H_{p^3} or an invariant H_{q^2}.*

G_{392}. The H_7 common to the $8H_{49}$ is invariant in the G_{392}, corresponding to which we have the factor group Γ_{56}. Since the supposed G_{392} has $8H_{49}$ the Γ_{56} has $8H_7$ and hence Γ_{56} has $1H_8$ leading to an invariant H_{56} in the G_{392}. This H_{56} must have $7H_8$, for if it had an invariant H_8 this H_8 would be invariant in the G_{392}, contrary to hypothesis. Now these $7H_8$ are the only H_8 in G_{392} and two of them have in common an H_4 which is invariant in the H_{56}. Hence the $7H_8$ have an H_4 in common which is invariant in the G_{392}. This gives us a factor group Γ_{98} which has $1H_{49}$, corresponding to which our G_{392} has an invariant H_{196}. This H_{196} contains only $1H_{49}$ and hence the latter is invariant in the G_{392}. There is then no type of G_{392} in our supposed case.

The treatment of G_{108} and G_{72}, in the case under consideration, will be given under division IV.

II.

$G_{p^3q^2}$ HAVING AN INVARIANT H_{q^2} AND MORE THAN ONE H_{p^3}.

Note. In the following T is an element of order q^2, while T_1, T_2 are elements of order q.

3. *General considerations. If there are* qH_{p^3}, then H_{q^2} must contain an H_q each element of which is commutative with an H_{p^3}. If now T_1 or T^q, according as H_{q^2} is non-cyclic or cyclic, is such an element and A any non-identical element of H_{p^3}, while B is a properly chosen element of H_{p^3}, then

and $$T_1^{-1}AT_1 = B$$

Hence $$T_1^{-1}AT_1A^{-1} = BA^{-1} = 1\,.$$

$$T_1^{-1}AT_1 = A\,.$$

It follows then that T_1 is commutative with each element of an H_{p^3}. If the H_{q^2} is cyclic, then just as above

$$A^{-1}T^qA = T^q.$$

Since $\{T\}$ is invariant we also have

$$A^{-1}TA = T^a.$$

Therefore $$A^{-1}T^qA = T^{aq} = T^q.$$

Hence $$aq = q \pmod{q^2}$$

or $$a = kq + 1$$

and since A is of order p, p^2 or p^3, we must have from the above

$$(kq+1)^p, \qquad (kq+1)^{p^2} \qquad \text{or} \qquad (kq+1)^{p^3} \equiv 1 \pmod{q^2}.$$

Each of these three cases requires that $k \equiv 0 \pmod{q}$ and hence

$$a \equiv 1 \pmod{q^2}.$$

This makes A and T commutative contrary to the hypothesis that there is more than $1H_{p^3}$. *Hence the case of* qH_{p^3} *and an invariant cyclic* H_{q^2} *cannot occur.*

If there are $q^2H_{p^3}$ we may have either

$$q \equiv 1 \pmod{p} \qquad \text{or} \qquad q \equiv -1 \pmod{p}.$$

If $p = 2$ these two congruences are identical.

We will take the different types of H_{p^3} and discuss all possible $G_{p^3q^2}$ obtained with each type.

4. *H_{p^3} cyclic, that is,* $A^{p^3}=1$.

(i) Let there be qH_{p^3}. Here

$$q \equiv 1 \pmod{p}.$$

The H_{q^2} must be non-cyclic (§ 3) and hence

$$T_1 A = A T_1.$$

Besides $\{T_1\}$ there are q other H_q in our invariant H_{q^2}. These qH_q may be divided into l sets of p, p^2 or p^3 each, the groups of each set being permuted cyclically by A; there will remain mH_q, each of which is invariant under A. Hence at least one of these qH_q is invariant under A, so that we may assume

$$A^{-1}T_2A = T_2^a.$$

We may now have three types of $G_{p^3q^2}$ according as a is a primitive root of one of the three following congruences:

$$a^p \equiv 1 \pmod{q}, \qquad a^{p^2} \equiv 1 \pmod{q}, \quad a^{p^3} \equiv 1 \pmod{q}.$$

Each group thus formed is the direct product of $\{A, T_2\}$ and $\{T_1\}$. The H_{p^3} have in common an H_{p^2}, H_p and H_1 respectively.

(ii) Let us take $q^2H_{p^3}$ and $q \equiv 1 \pmod{p}$.

For cyclic H_{q^2} $A^{-1}TA = T^a$.

Again we have three types of $G_{p^3q^2}$ according as a is a primitive root of one of the three congruences:

$$a^p \equiv 1 \pmod{q^2}, \qquad a^{p^2} \equiv 1 \pmod{q^2}, \qquad a^{p^3} \equiv 1 \pmod{q^2}.$$

Non-cyclic H_{q^2}. If $p > 2$, then since

$$q \equiv 1 \pmod{p}$$

we have
$$q+1 \equiv 2 \pmod{p}.$$

Hence by the same reasoning as in (i) $2H_q$ are each invariant under A. However when $p=2$ there may be no H_q invariant under A. In every case, if there is one H_q invariant under A there will be at least two.

We will first consider the case in which $p=2$ and there is no H_q invariant in $G_{p^3q^2}$. Hence we may assume

$$A^{-1}T_1A = T_2$$

and
$$A^{-1}T_2A = T_1^aT_2^b.$$

A^2 cannot be permutable with T_1, for then $\{T_1T_2\}$ would be invariant in $G_{p^3q^2}$.

If A^4 is the lowest power of A permutable with T_1, then

$$A^{-1}T_1A = T_2,$$
$$A^{-2}T_1A^2 = A^{-1}T_2A = T_1^aT_2^b,$$
$$A^{-3}T_1A^3 = A^{-2}T_2A^2 = T_1^{ab}T_2^{a+b^2},$$
$$T_1 = A^{-4}T_1A^4 = A^{-3}T_2A^3 = T_1^{a^2+ab^2}T_2^{2ab+b^3}.$$

Hence we must have the congruences

$$\left.\begin{aligned} a^2 + ab^2 &\equiv 1 \\ b(2a + b^2) &\equiv 0 \end{aligned}\right\} \pmod q.$$

The solution $b \equiv 0$, $a \equiv +1$ has already been excluded since it makes T_1 permutable with A^2. The solution $b \equiv 0$, $a \equiv -1$ gives one type of G_{8q^2}. In this G_{8q^2} every H_q is invariant in an $H_{4q^2} = \{A^2, T_1, T_2\}$.

Since we suppose there is no H_q invariant in our G_{8q^2}, then if x is a Galoisian imaginary, we have

(1) $$A^{-1}T_1^\alpha T_2^\beta A = (T_1^\alpha T_2^\beta)^x = T_1^{\alpha x}T_2^{\beta x},$$

that is, there exists no real number x which will satisfy the above equation $(\alpha, \beta = 0, 1, 2, 3, \cdots, q-1)$. Since

$$A^{-1}T_1A = T_2$$

and $$A^{-1}T_2A = T_1^{-1}$$

we have $$A^{-1}T_1^\alpha T_2^\beta A = T_1^{-\beta}T_2^\alpha.$$

Comparing exponents in (1) and above we have

$$\alpha x \equiv -\beta, \qquad \beta x \equiv \alpha \pmod q,$$

whence $$x^2 \equiv -1 \pmod q.$$

Since x cannot be a real number q must be of the form $4m + 3$.

Again if $$2a + b^2 \equiv 0 \pmod q$$

and, therefore, $$b^2 \equiv -2a \pmod q.$$

We have $$a^2 \equiv -1 \pmod q.$$

Hence

(2) $$a^2b^2 \equiv 2a \pmod q.$$

Now

(3) $$A^{-1}T_1^\alpha T_2^\beta A = T_1^{a\beta}T_2^{\alpha+b\beta}.$$

From (1) and (3) we have

$$\alpha\beta \equiv \alpha x, \qquad \alpha + b\beta \equiv \beta x \pmod q$$

and hence we get $$x^2 - bx \equiv a \pmod q,$$
whence

(4) $$(2x-b)^2 = 4(x^2 - bx) + b^2 \equiv 2a \pmod q.$$

But from (2), $2a$ is a quadratic remainder and hence real values of x exist which will satisfy (4) contrary to the hypothesis that x is not real. Hence the supposition $2a + b^2 \equiv 0 \pmod q$ does not lead to a type of $G_{p^3q^2}$.

Suppose, then, A^8 is the lowest power of A commutative with any element of H_{q^2}, say T_1; and suppose first that

$$A^{-4}T_1A^4 = T_2,$$

that is, T_1 is not transformed into a power of itself by A^4. Hence

$$A^{-8}T_1A^8 = A^{-4}T_2A^4 = T_1.$$

Therefore $$A^{-4}T_1T_2A^4 = T_1T_2.$$

If T_1 is put in place of T_1T_2 we will have

$$A^{-4}T_1A^4 = T_1$$

contrary to hypothesis. It follows, then, that A^4 transforms T_1 into one of its powers. Therefore

$$A^{-4}T_1A^4 = T_1^{-1}.$$

Let $$A^{-1}T_1A = T_2$$

and $$A^{-1}T_2A = T_1^aT_2^b.$$

Hence we must have the congruences

(5) $$a^2 + ab^2 \equiv -1, \qquad b(2a+b^2) \equiv 0 \pmod q.$$

If $$b \equiv 0 \qquad \text{then} \qquad a^2 \equiv -1.$$

Hence q is of the form $4m+1$ since a is real; a is a primitive root of

$$a^4 \equiv 1 \pmod q.$$

This gives one type of G_{8q^2}. Each H_q is invariant in a $G_{4q^2} = \{A^2, T_1, T_2\}$.

If $$b^2 + 2a \equiv 0,$$

then from (5) $$a^2 \equiv 1.$$

But from (4) $$(2x-b)^2 \equiv 2a.$$

We must now consider two cases according as $a \equiv +1$ or -1. If

$$a \equiv 1,$$

then we have the congruences

$$b^2 \equiv -2, \qquad (2x-b)^2 \equiv 2 \pmod q.$$

Since x is not real q is of the form $8n+3$. The former congruence has only one pair of roots. That each of these roots furnishes the same type of group may be established as follows. Let us take the relations

$$A^{-1}T_1A = T_2, \qquad A^{-1}T_2A = T_1T_2^b$$

and change generators by setting

$$A_0 = A^5, \qquad T_3 = T_1, \qquad T_4 = T_2^{-1}$$

so that our $$G_{p^3q^2} = \{A_0,\, T_3,\, T_4\}.$$

Hence $$A_0^{-1}T_3A_0 = T_4, \qquad A_0^{-1}T_4A_0 = T_3T_4^{-b}.$$

If $$a \equiv -1,$$
we have the congruences

$$b^2 \equiv 2, \qquad (2x-b)^2 \equiv -2 \pmod q.$$

Hence q is of the form $8n+7$. Here again we get a single type of group.

Suppose

(6) $$A^{-1}T_1A = T_1^a \qquad \text{then also} \qquad A^{-1}T_2A = T_2^b;$$

neither a nor b can be unity.

If $p > 2$ then p cannot divide $q+1$ and hence we must inevitably have relations of the form (6). We may now have the following cases: a and b both primitive roots of

(α) $$z^p \equiv 1 \pmod q.$$

(β) $$z^{p^2} \equiv 1.$$

(γ) $$z^{p^3} \equiv 1.$$

(δ) a a primitive root of $z^p \equiv 1$ while b is a primitive root of $z^{p^2} \equiv 1$.

(ϵ) a as in (δ) while b is a primitive root of $z^{p^3} \equiv 1$.

(ζ) a a primitive root of $z^{p^2} \equiv 1$ with b as in (ϵ).

As regards the three cases (α) (β) (γ) relations (6) may be written

$$A^{-1}T_1A = T_1^a, \qquad A^{-1}T_2A = T_2^{a^x} \qquad (x \text{ prime to } p).$$

Transforming with A^y in place of A, where y is prime to p,

$$A^{-y}T_1A^y = T_1^{a^y}, \qquad A^{-y}T_2A^y = T_2^{a^{xy}}.$$

If y is so taken that

$$xy \equiv 1 \pmod{p}, \qquad 1 \pmod{p^2}, \qquad 1 \pmod{p^3}$$

for the three cases respectively, we have the same relations as before with y in place of x and with T_2 in place of T_1. Hence the number of types is the number of solutions of the three above congruences, the solutions (x_1, y_1) being regarded the same as the solution (y_1, x_1). Therefore in
case (α) the number of types is $(p+1)/2$ for p odd and a single type for $p = 2$,
case (β) the number of types is $(p^2 - p + 2)/2$ for p odd or even,
case (γ) the number of types is $(p^3 - p^2 + 2)/2$ for p odd and four types for $p = 2$. If $x = 1$ in these three cases, all the $(q+1)H_q$ of our invariant H_{q^2} are invariant in the whole $G_{p^3q^2}$. In case (δ) there are $p - 1$ types, since b may be fixed as any one of the primitive roots of $x^{p^2} \equiv 1 \pmod{q}$ and there are $p - 1$ types corresponding to the $p-1$ values of a. In like manner case (ϵ) furnishes $p - 1$ types and case $(\zeta)\, p(p-1)$ types.

5. $q^2H_{p^3}$ and $q \equiv -1 \pmod{p}$. Here we will take $p > 2$, for the case $p = 2$ has already been treated in § 4. A cannot transform T_1 into one of its powers, for if we had

$$A^{-1}T_1 = T_1^a,$$

then since $a \not\equiv 1 \pmod{q}$ it would have to be a primitive root of x^p, x^{p^2} or $x^{p^3} \equiv 1 \pmod{q}$. Clearly this is impossible. We must therefore have the relations:

$$A^{-1}T_1A = T_2, \qquad A^{-1}T_2A = T_1^aT_2^b.$$

Using Galoisian imaginaries we may write

$$A^{-1}T_1A = T_1^i.$$

Proceeding as Burnside does in his *Theory of Groups*, pp. 136–7, we see that there are three types of groups in our case according as i belongs to the exponent p, exponent p^2 or exponent $p^3 \pmod{q}$, that is, according as A^p, A^{p^2} or A^{p^3} is the lowest power of A permutable with T_1. The second and third cases require $q \equiv -1 \pmod{p^2}$ and $q \equiv -1 \pmod{p^3}$ respectively. Here $a \equiv -1$ and $b \equiv i^q + i \pmod{q}$.

I give the following illustration of the use of Galoisian imaginaries for finding b in the case where i is a primitive root of the congruence

$$i^p \equiv 1 \pmod{q}.$$

Let us take a $G_{p^3q^2} = G_{5^3 \cdot 19^2}$. Since 2 is quadratic non-remainder (mod 19) we form the irreducible function

$$F(x) = x^2 - 2.$$

Cf. HÖLDER, Mathematische Annalen, vol. 43, pp. 350–1; also DICKSON, *Linear Groups*, § 6.

We must now find a function $f(x)$, i. e., a mark of our Galois field (cf. DICKSON, *Linear Groups*, p. 7), such that

$$[f(x)]^5 \equiv 1 \quad \{\text{mod}\,[19, x^2-2]\}.$$

The period of our mark is 5 and is a divisor of $19^2 - 1$ (cf. DICKSON, loc. cit., p. 11). To obtain this mark we proceed by trial.

(1) The different powers of x mod $[19, x^2 - 2]$ are

$$\begin{array}{cccccccccccc} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, & 11, & 12, \\ x, & 2, & 2x, & 4, & 4x, & 8, & 8x, & 16, & 16x, & -6, & -6x, & 7, \\ \hline & & & 13, & 14, & 15 & & 16, & 17, & 18, & & \\ & & & 7x, & 14, & 14x, & & 9, & 9x, & -1. & & \end{array}$$

Hence $$x^{36} \equiv 1 \quad \{\text{mod}\,[19, x^2-2]\},$$

that is, the mark x belongs to the exponent 36 and since 36 is not divisible by 5, none of the powers of x given above can be taken as our mark of period 5.

(2) Let us now try the powers of $1 + x$ mod $[19, x^2 - 2]$,

$$\begin{array}{cccccccc} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, \\ 1+x, & 3+2x, & 5x+7, & -2-7x, & 3+10x, & 13x+4, & 2x+11, & 9x+7, \\ \hline 9, & 10, & \cdots, & 20, & \cdots, & 40, & & \\ -3x+6, & 3x, & \cdots, & -1, & \cdots, & +1. & & \end{array}$$

Hence $$[(1+x)^8]^5 \equiv 1 \quad \{\text{mod}\,[19, x^2-2]\},$$

that is $$(9x+7)^5 \equiv 1 \quad \{\text{mod}\,[19, x^2-2]\}.$$

We take $$i \equiv 9x + 7 \quad \{\text{mod}\,[19, x^2-2]\},$$

and hence $i^q = i^{19} = (7+9x)^4 \equiv 7 + 10x \quad \{\text{mod}\,[19, x^2-2]\}$,

and $$b = i + i^q = 19x + 14 \equiv 14.$$

Hence our $G_{5^3 . 19^2}$ is defined by the relations:

$$A^{125} = T_1^{19} = T_2^{19} = 1, \qquad A^{-1}T_1A = T_2, \qquad A^{-1}T_2A = T_1^{18}T_2^{14}, \qquad T_1T_2 = T_2T_1.$$

The result obtained above may be verified as follows. Let us represent an isomorphism of $\{T_1, T_2\}$ which is invariant in the whole group by

$$J = \begin{pmatrix} T_1 & T_2 \\ T_2 & T_1^{-1}T_2^b \end{pmatrix}.$$

This is the transformation of $\{T_1, T_2\}$ under the element A.

$$J^2 = \begin{pmatrix} T_1, & T_2 \\ T_1^{-1} T_2^{b}, & T_1^{-b} T_2^{b^2-1} \end{pmatrix},$$

$$J^3 = \begin{pmatrix} T_1, & T_2 \\ T_1^{-b} T_2^{b^2-1}, & T_1^{-(b^2-1)} T_2^{b^3-2b} \end{pmatrix},$$

$$J^4 = \begin{pmatrix} T_1, & T_2 \\ T_1^{-(b^2-1)} T_2^{b^3-2b}, & T_1^{-(b^3-2b)} T_2^{b^4-3b^2+1} \end{pmatrix},$$

$$J^5 = \begin{pmatrix} T_1, & T_2 \\ T_1^{-(b^3-2b)} T_2^{b^4-3b^2+1}, & T_1^{-(b^4-3b^2+1)} T_2^{b^5-4b^3+3b} \end{pmatrix}.$$

Since J^5 is here the identical isomorphism, we must have the two congruences

$$b^4 - 3b^2 + 1 \equiv 0 \pmod{19}, \qquad -b^3 + 2b \equiv 1 \pmod{19}.$$

By trial we find that these two congruences are satisfied by $b \equiv 14$, and from the method of forming these isomorphisms it is evident that $b = 14$ will also satisfy the congruence

$$b^5 - 4b^3 + 3b \equiv 1 \pmod{19}.$$

6. $$H_{p^3} = \{A^{p^2} = B^p = 1, \qquad AB = BA\}.$$

(i) Let there be qH_{p^3}. Therefore $q \equiv 1 \pmod{p}$. The H_{q^2} is non-cyclic (§ 3) and hence we may assume the relations:

$$A^{-} T_1 A = T_1, \qquad B^{-1} T_1 B = T_1, \qquad A^{-1} T_2 A = T_2^{a}, \qquad B^{-1} T_2 B = T_1^{\beta} T_2^{b}.$$

Therefore $$B^{-1} A^{-1} T_1 T_2 AB = T_1^{1+a\beta} T_2^{ab},$$

and $$A^{-1} B^{-1} T_1 T_2 BA = T_1^{1+\beta} T_2^{ab}.$$

Since $AB = BA$, we have the congruence

$$1 + a\beta \equiv 1 + \beta.$$

Hence $$a \equiv 1 \qquad \text{or} \qquad \beta \equiv 0.$$

In the former case A is permutable with each of the $q + 1 H_q$ of H_{q^2}, and as B is permutable with two of them, there exists at least $2H_q$ invariant in the whole $G_{p^3q^2}$. Hence we have the relations:

$$A^{-1} T_1 A = T_1, \qquad B^{-1} T_1 B = T_1, \qquad A^{-1} T_2 A = T_2^{a}, \qquad B^{-1} T_2 B = T_2^{b}.$$

If $a \equiv 1 \pmod{q}$ and b belongs to the exponent $p \pmod{q}$ we get one $G_{p^3q^2}$ which is the direct product of $\{T_1, A\}$ and $\{B, T_2\}$. The qH_{p^3} have in common an $H_{p^2} = \{A\}$. If $b \equiv 1$ our $G_{p^3q^2}$ is the direct product of $\{B, T\}$ and

$\{A, T_2\}$. Here we get two types according as a belongs to the exponent p or exponent p^2 (mod q). In the former case the H_{p^3} have in common an $H_{p^2} = \{A^p, B\}$, while in the latter case they have in common an $H_p = \{B\}$.

If a and b belong to the exponent p (mod q) we set $b = a^y$ and we can then put in place of A, $A_0 = A^x B$ (x prime to p), keeping B fixed, and therefore

$$A_0^{-1} T_2 A_0 = B^{-1} A^{-x} T_2 A^x B = T_2^{a^{x+y}}.$$

If x is so chosen that

$$x + y = 0$$

this case reduces to one in which $a \equiv 1$. Again if a belongs to the exponent p^2 and b to the exponent p (mod q) we may set $a^p = b^z$. We next keep A fixed and in place of B put $B_0 = A^p B^r$ (r prime to p). Hence

$$B_0^{-1} T_2 B_0 = B^{-r} A^{-p} T_2 A^p B^r = T_2^{b^{z+r}}.$$

If r is so chosen that

$$z + r = 0$$

this case reduces to one in which $b \equiv 1$.

(ii) Suppose there are $q^2 H_{p^3}$ and also $q \equiv 1 \pmod p$.

For *cyclic* H_{q^2} we have the relations

$$A^{-1} TA = T^a, \qquad B^{-1} TB = T^b.$$

Just as in the preceding we get three types of groups. Two of them are the direct products of $\{B\}$ and $\{T, A\}$; the other is the direct product of $\{A\}$ and $\{T, B\}$.

If $p > 2$, then for H_{q^2} *non-cyclic* we may always assume the relations:

(*a*) $A^{-1}T_1A = T_1^a, \quad B^{-1}T_1B = T_1^b, \quad A^{-1}T_2A = T_2^\alpha, \quad B^{-1}T_2B = T_2^\beta.$

For suppose there is only $1 H_q$, say $\{T_1\}$ invariant in our $G_{p^3q^3}$, then

(*b*) $A^{-1}T_1A = T_1^a, \quad B^{-1}T_1B = T_1^b, \quad A^{-1}T_2A = T_2^\alpha, \quad B^{-1}T_2B = T_1^\beta T_2^\gamma.$

Hence

$$B^{-1}A^{-1}T_1T_2AB = T_1^{ab+\alpha\beta} T_2^{\alpha\gamma} = A^{-1}B^{-1}T_1T_2BA = T_1^{ab+a\beta} T_2^{\alpha\gamma}.$$

Therefore $\beta \equiv 0$ or $a \equiv \alpha$ and accordingly relations (*b*) reduce to (*a*) just as in (i) above. Again suppose there is no H_q invariant in $G_{p^3q^3}$. Then we have relations:

(*c*) $A^{-1}T_1A = T_1^a, \quad B^{-1}T_1B = T_1^b T_2^c, \quad A^{-1}T_2A = T_2^\alpha, \quad B^{-1}T_2B = T_1^\beta T_2^\gamma.$

Now $$B^{-1}A^{-1}T_1T_2AB = T_1^{ab+\alpha\beta} T_2^{ac+\alpha\gamma},$$

and $$A^{-1}B^{-1}T_1T_2BA = T_1^{ab+a\beta} T_2^{\alpha c+\alpha\gamma},$$

whence $\beta \equiv 0$ or $\alpha \equiv a$ and accordingly relations (*c*) reduce to (*a*).

In (a) we cannot have $\alpha \equiv \beta \equiv 1$ or $a \equiv b \equiv 1$, for then there would be only qH_{p^3}. Just as in (i) above we can make one of the exponents $a, b, \alpha, \beta \equiv 1$.

(1) If $\alpha \equiv b \equiv 1$ we get two types according as a belongs to the exponent p or exponent p^2 (mod q).

(2) If $\alpha \equiv a \equiv 1$ we get $(p+1)/2$ types, each being the direct product of $\{A\}$ and $\{B, T_1, T_2\}$. With regard to the last named subgroup see HÖLDER, Mathematische Annalen, Vol. 43, pp. 341–45.

(3) If $b \equiv \beta \equiv 1$ each $G_{p^3q^2}$ is the direct product of $\{B\}$ and $\{A, T_1, T_2\}$ and, therefore, we have three cases (cf. LEVAVASSEUR, l. c., pp. 339–41).

(α) If a and α both belong to the exponent p (mod q) there are $(p+1)/2$ types.

(β) If a and α both belong to the exponent p^2 (mod q) there are $(p^2-p+2)/2$ types.

(γ) If a belongs to the exponent p while α belongs to the exponent p^2 (mod q), there are $p-1$ types.

(4) If $\alpha \equiv 1$; $a, b, \beta \not\equiv 1$ and a belongs to the exponent p (mod q) we get $(p+1)/2$ types. If a belongs to the exponent p^2, this case reduces to one of the preceding.

(5) If $\beta \equiv 1$; $\alpha, a, b \not\equiv 1$ then to get new types we must have a belonging to the exponent p^2 (mod q). If a belongs to the exponent p^2 (mod q) we get $(p^2-p+2)/2$ types, while if α belongs to the exponent p (mod q) we get $p-1$ types.

If $p=2$, B must transform some element of H_{q^2}, say T_1, into one of its powers; and, therefore, a second element, say T_2, into one of its powers also.

Hence $$B^{-1}T_1B = T_1^{\alpha}, \qquad B^{-1}T_2B = T_2^{\beta}.$$

If we also have $$A^{-1}T_1A = T_1^{a}$$

then we can apply treatment similar to the above for $p > 2$. But if

$$A^{-1}T_1A = T_2$$

and hence $$A^{-1}T_2A = T_1^{a}T_2^{b},$$

then proceeding just as in § 4, where $p=2$ and A^4 is the lowest power of A permutable with T_1, we find $b \equiv 0$ and $a \equiv -1$. If $\alpha \equiv \beta \equiv +1$ we get one type of G_{8q^2} which is the direct product of $\{B\}$ and $\{A, T_1, T_2\}$. As in § 4 q must be of the form $4m+3$. There can be no other type with the relations

$$A^{-1}T_1A = T_2, \qquad B^{-1}T_1B = T_1^{\alpha}, \qquad A^{-1}T_2A = T_1^{-1}, \qquad B^{-1}T_2B = T_2^{\beta},$$

For $$B^{-1}A^{-1}T_1T_2AB = T_2^{\beta}T_1^{-\alpha}$$

and $$A^{-1}B^{-1}T_1T_2BA = T_2^{\alpha}T_1^{-\beta}.$$

Hence $$\beta \equiv \alpha \equiv \pm 1.$$

If, however, we take $\alpha \equiv \beta \equiv -1$, we can keep A fixed and set $B_0 = A^2B$ in place of B so that

$$B_0^{-1}T_1B_0 = B^{-1}A^{-2}T_1A^2B = T_1.$$

Hence the value -1 for α and β gives the same type as $+1$.

7. $q^2H_{p^3}$, and $q \equiv -1 \pmod p$ $(p > 2)$. Neither A nor B can transform any element of our non-cyclic H_{q^2}, say T_1, into one of its powers different from unity. For if we had

$$A^{-1}T_1A = T_1^a \qquad \text{or} \qquad B^{-1}T_1B = T_1^b \qquad (a, b \neq 1)$$

we would have $q \equiv 1 \pmod p$ which is impossible. We may have the relations:

$$A^{-1}T_1A = T_2, \qquad A^{-1}T_2A = T_1^aT_2^b, \qquad B^{-1}T_1B = T_1, \qquad B^{-1}T_2B = T_2.$$

These give two types of $G_{p^3q^2}$, each being the direct product of $\{A, T_1, T_2\}$ and $\{B\}$. The exponents a and b are determined as in § 5.

We may also have the relations:

$$A^{-1}T_1A = T_1, \qquad A^{-1}T_2A = T_2, \qquad B^{-1}T_1B = T_2, \qquad B^{-1}T_2A = T_1^\alpha T_2^\beta,$$

α and β satisfying the same relations as a and b for the corresponding case in § 5. This gives one type of $G_{p^3q^2}$, the direct product of $\{A\}$ and $\{B, T_1, T_2\}$.

The hypothesis that no element of $\{A, B\}$ is permutable with an H_q of $\{T_1, T_2\}$ is inadmissible. This follows from the discussion of the isomorphisms of the non-cyclic H_{q^2} by LEVAVASSEUR in his *Enumération des Groupes d'Operations d'Ordre donnée*, p. 52. The conclusion of this discussion is stated in his article on $G_{p^2q^2}$, loc. cit., p. 349, as follows: "The substitutions with characteristic irreducible congruences* divide into cyclic groups J† forming a complete and unique series of conjugate subgroups; then two isomorphisms corresponding to two such substitutions can only be permutable if the one is a power of the other." From the above it is evident that no type of $G_{p^3q^2}$ with cyclic H_{q^2} exists in our supposed case.

8. $H_{p^3} = \{A^p = B^p = C^p = 1, \quad AB = BA, \quad AC = CA, \quad BC = CA\}$.

(i) Suppose there are qH_{p^3} and hence $q \equiv 1 \pmod p$. The H_{q^2} is non-cyclic and the most general form of our relations is

$$A^{-1}T_1A = T_1, \qquad B^{-1}T_1B = T_1, \qquad C^{-1}T_1C = T_1,$$
$$A^{-1}T_2A = T_2^a, \qquad B^{-1}T_2B = T_1^\beta T_2^b, \qquad C^{-1}T_2C = T_1^\gamma T_2^c.$$

* Cf. HÖLDER, Mathematische Annalen, vol. 43, pp. 348–9; also BURNSIDE, *Theory of Groups*, p. 136.

† See § 5 for this J.

On transforming T_1T_2 by $AB=BA$ as in § 6 we see that we may assume $\beta\equiv 0$. Next on transforming T_1T_2 with $AC=CA$ we have either $a\equiv 1$ or $\gamma\equiv 0$. If $a\equiv 1$ we then transform T_1T_2 with $BC=CB$ and thus find that $b\equiv 1$ or $\gamma\equiv 0$, so that we may assume the relations:

$$A^{-1}T_1A=T_1,\qquad B^{-1}T_1B=T_1,\qquad C^{-1}T_1C=T_1$$
$$A^{-1}T_2A=T_2^a,\qquad B^{-1}T_2B=T_2^b,\qquad C^{-1}T_2C=T_2^c.$$

If $a,\,b,\,c\not\equiv 1$ then by the same process as in § 6 where a and b both belong to the exponent $p\ (\mathrm{mod}\ q)$ we can make $a\equiv 1$. Then keeping A fixed we can repeat the process so as to make $b\equiv 1$. Hence we may assume $a\equiv b\equiv 1$ while c must belong to the exponent $p\ (\mathrm{mod}\ q)$, so that we get one type of $G_{p^3q^2}$ which is the direct product of $\{T_1\}\ \{A\}\ \{B\}$ and $\{C,\,T_2\}$. The H_{p^3} have in common an $H_{p^2}=\{A,\,B\}$.

(ii) Suppose there are $q^2H_{p^3}$ and also $q\equiv 1\ (\mathrm{mod}\ p)$. If the H_{q^2} is cyclic we have the relations

$$A^{-1}TA=T^a,\qquad B^{-1}TB=T^b,\qquad C^{-1}TC=T^c.$$

By proper change of generators, just as above, we can assume $a\equiv b\equiv 1$ and hence we get a single type.

For H_{q^2} non-cyclic we make the following suppositions.

(1) Let the H_{q^2} contain at least $2H_q$ with each of which A, B and C are commutative. Hence we have

$$A^{-1}T_1A=T_1^a,\qquad B^{-1}T_1B=T_1^b,\qquad C^{-1}T_1C=T_1^c$$
$$A^{-1}T_2A=T_2^\alpha,\qquad B^{-1}T_2B=T_2^\beta,\qquad C^{-1}T_2C=T_2^\gamma.$$

As above we can make two of the exponents $a,\,b,\,c\equiv 1$, say a and b. Then after that we can make one of the exponents α or $\beta\equiv 1$. The above relations then take the form

$$A^{-1}T_1A=T_1,\qquad B^{-1}T_1B=T_1,\qquad C^{-1}T_1C=T_1^c$$
$$A^{-1}T_2A=T_2,\qquad B^{-1}T_2B=T_2^\beta,\qquad C^{-1}T_2C=T_2^\gamma,$$

Hence these groups are always decomposable. If $\beta\equiv 1$ we get $(p+1)/2$ types [c.f. § 4 (ii), case (α)] which are the direct products of $\{A,\,B\}$ and $\{C,\,T_1,\,T_2\}$. If $\gamma\equiv 1$, $\beta\not\equiv 1$ we get a type of $G_{p^3q^2}$ which is the direct product of $\{T_1,\,C\}$ and $\{T_2,\,B\}$. If $c,\,\beta,\,\gamma$, are different from unity we can, by a proper change of generators, reduce to one of the preceding cases.

(2) Suppose there is only one H_q invariant in the whole $G_{p^3q^2}$. Let this H_q be generated by T_1. We may take the element A commutative with $\{T_2\}$ and, therefore, we have the relations

$$A^{-1}T_1A=T_1^a,\qquad B^{-1}T_1B=T_1^b,\qquad C^{-1}T_1C=T_1^c,$$
$$A^{-1}T_2A=T_2^\alpha,\qquad B^{-1}T_2B=T_1^lT_2^\beta,\qquad C^{-1}T_2C=T_1^mT_2^\gamma.$$

We now transform and make use of the fact that $AB = BA$.

$$B^{-1}A^{-1}T_1T_2AB = B^{-1}T_1^{a}T_2^{\alpha}B = T_1^{ab+l\alpha}T_2^{\alpha\beta}$$

and
$$A^{-1}B^{-1}T_1T_2BA = A^{-1}T_1^{b+l}T_2^{\beta}A = T_1^{ab+la}T_2^{\alpha\beta}.$$

Hence $l \equiv 0$ or $a \equiv \alpha$. In the latter case A would be commutative with all the $(q+1)H_q$ and as B is commutative with two of them, we may now write our relations in the form

$$\begin{array}{lll} A^{-1}T_1A = T_1^{a}, & B^{-1}T_1B = T_1^{b}, & C^{-1}T_1C = T_1^{c}, \\ A^{-1}T_2A = T_2^{\alpha}, & B^{-1}T_2B = T_2^{\beta}, & C^{-1}T_2C = T_1^{m}T_2^{\gamma}. \end{array}$$

Transform, making use of $AC = CA$ just as above. Then $a \equiv \alpha$, since $m \equiv 0$ makes $2H_q$ invariant in $G_{p^3q^3}$ contrary to hypothesis. Again transform, using $BC = CB$. This makes $b \equiv \beta$. Since $a \equiv \alpha$ and $b \equiv \beta$ all the H_q are permutable with A and B, and since $2H_q$ are permutable with C, we find that the case of only one H_q invariant in $G_{p^3q^3}$ is impossible.

(3) Suppose there is no H_q invariant in our $G_{p^3q^3}$. On account of the congruence

$$q \equiv 1 \pmod{p}$$

$2H_q$ must be commutative with A, $2H_q$ commutative with B, and $2H_q$ commutative with C. Our relations may now be written

$$\begin{array}{lll} A^{-1}T_1A = T_1^{a}, & B^{-1}T_1B = T_1^{\gamma}T_2^{\delta}, & C^{-1}T_1C = T_1^{b}T_2^{c}, \\ A^{-1}T_2A = T_1^{\alpha}T_2^{g}, & B^{-1}T_2B = T_2^{\beta}, & C^{-1}T_2C = T_1^{l}T_2^{m}. \end{array}$$

Let us transform as follows:

$$B^{-1}A^{-1}T_2AB = B^{-1}T_1^{\alpha}T_2^{g}B = T_1^{\alpha\gamma}T_2^{\alpha\delta+g\beta}$$

and
$$A^{-1}B^{-1}T_2BA = A^{-1}T_2^{\beta}A = T_1^{\alpha\beta}T_2^{g\beta}.$$

Hence $\alpha\delta \equiv 0$, so that either $\alpha \equiv 0$ or $\delta \equiv 0$, and proceeding as in (2) above we see that our relations may be written in the form

$$\begin{array}{lll} A^{-1}T_1A = T_1^{a}, & B^{-1}T_1B = T_1^{b}, & C^{-1}T_1C = T_1^{c}T_2^{d}, \\ A^{-1}T_2A = T_2^{\alpha}, & B^{-1}T_2B = T_2^{\beta}, & C^{-1}T_2C = T_1^{\gamma}T_2^{\delta}. \end{array}$$

Again let us transform thus,

$$B^{-1}C^{-1}T_2CB = B^{-1}T_1^{\gamma}T_2^{\delta}B = T_1^{b\gamma}T_2^{\beta\delta},$$

and
$$C^{-1}B^{-1}T_2BC = C^{-1}T_2^{\beta}C = T_1^{\beta\gamma}T_2^{\beta\delta}.$$

Whence $b \equiv \beta$, since $\gamma \not\equiv 0$; for otherwise $1H_q$ would be invariant in the whole group. Using A and C we can show $a \equiv \alpha$. Hence just as in (2) hypothesis (3) is absurd.

9. $q^2 H_{p^3}$ and $q \equiv -1 \pmod{p}$ $(p > 2)$. We may have one type of G_{p^3q} defined by the relations:

$$A^{-1}T_1A = T_2, \qquad B^{-1}T_1B = T_1, \qquad C^{-1}T_1C = T_1,$$
$$A^{-1}T_2A = T_1^{-1}T_2^b, \qquad B^{-1}T_2B = T_2, \qquad C^{-1}T_2C = T_2,$$

$b = i + i^q$ where i is a Galoisian imaginary. This $G_{p^3q^2}$ is the direct product of $\{A, T_1, T_2\}$ and $\{B, C\}$. There can be no other type in this case (§ 7).

10. H_{p^3} *of the type* $A^4 = B^2 = 1$, $B^{-1}AB = A^3$.

(i) Suppose there are qH_8. Hence the H_{q^2} are non-cyclic. Therefore

(§ 3) $$A^{-1}T_1A = T_1, \qquad B^{-1}T_1B = T_1.$$

Since B must be permutable with a second H_q, say $\{T_2\}$ we must have the relations

$$B^{-1}T_2B = T_2^{\beta}, \qquad A^{-1}T_2A = T_1^aT_2^b.$$

We transform making use of the relation $AB = BA^3$. Hence

$$B^{-1}A^{-1}T_1T_2AB = T^{1+a}T_2^{b\beta} = A^{-3}B^{-1}T_1T_2BA^3 = T_1^{1+a\beta(1+b+b^2)}T_2^{b^3\beta}.$$

Therefore we must have the congruences:

$$b\beta \equiv b^3\beta, \qquad a \equiv \beta a(1 + b + b^2) \pmod{q}.$$

β must have the values ± 1.

If $\beta \equiv 1$ all the H_q are commutative with B and hence we may assume $T_1^aT_2^b = T_2^a$.

If $\beta \equiv -1$ then $a \equiv -a(1 + b + b^2)$.

If $a \equiv 0$ the last congruence is satisfied and, therefore

$$A^{-1}T_2A = T_2^b.$$

Suppose $a \not\equiv 0$ then we must have $b \equiv \pm 1$. Hence we have two cases according as $b \equiv +1$ or $b \equiv -1$. Therefore

$$1 \equiv -1(1 + 1 + 1) \pmod{q},$$

or

$$1 \equiv -1(1 - 1 + 1) \pmod{q}.$$

Each of these congruences requires that q is divisible by 2, which is absurd. Our relations may now be written

$$A^{-1}T_1A = T_1, \qquad B^{-1}T_1B = T_1,$$
$$A^{-1}T_2A = T_2^b, \qquad B^{-1}T_2B = T_2^{\beta},$$

where b and β take the values ± 1, but both cannot be $+1$ under our supposition.

If $\quad b \equiv -1, \ \beta \equiv +1$ we get one type of G_{8q^2}.
If $\quad b \equiv +1, \ \beta \equiv -1$ we get another type of G_{8q^2}.
$b \equiv -1, \ \beta \equiv -1$ does not give a new type,

for AB in place of B leaves T_2 fixed. Both these types of G_{8q^2} are the direct products of $\{T_1\}$ and $\{T_2, A, B\}$.

(ii) q^2H_8. For the *cyclic* H_{q^2} we have the relations,

$$A^{-1}TA = T^a, \qquad B^{-1}TB = T^b.$$

Since $AB = BA^3$ we transform as follows;

$$B^{-1}A^{-1}TAB = T^{ab} = A^{-3}B^{-1}TBA^3 = T^{a^3b}.$$

Hence $\quad a \equiv \pm.$ Also $b \equiv \pm 1.$

If $\ a \equiv +1$ and $b \equiv -1$ we get a G_{8q^2} in which $\{A\}$ is invariant.
If $\ a \equiv -1$ and $b \equiv +1$ we get a G_{8q^2} in which $\{A\}$ is not invariant.
$a \equiv -1, \quad b \equiv -1$ gives the same type as the latter,

for we may take AB in place of B and then $b \equiv +1$.

Non-cyclic H_{q^2}.

(1) Suppose that H_{q^2} has $2H_q$ invariant in G_{8q^2}. Therefore

$$A^{-1}T_1A = T_1^a, \qquad B^{-1}T_1B = T_1^b, \qquad A^{-1}T_2A = T_2^\alpha, \qquad B^{-1}T_2B = T_2^\beta.$$

The same procedure as above shows that $a, \alpha \equiv \pm 1$. We accordingly get four types with the following relations:

(*a*) $A^{-1}T_1A = T_1^{-1}, \quad B^{-1}T_1B = T_1, \quad A^{-1}T_2A = T_2^{-1}, \quad B^{-1}T_2B = T_2.$

(*b*) $A^{-1}T_1A = T_1, \quad B^{-1}T_1B = T_1^{-1}, \quad A^{-1}T_2A = T_2, \quad B^{-1}T_2B = T_2^{-1}.$

(c) $A^{-1}T_1A = T_1^{-1}, \quad B^{-1}T_1B = T_1, \quad A^{-1}T_2A = T_2^{-1}, \quad B^{-1}T_2B = T_2^{-1}.$

(*d*) $A^{-1}T_1A = T_1^{-1}, \quad B^{-1}T_1B = T_1, \quad A^{-1}T_2A = T_2, \quad B^{-1}T_2B = T_2^{-1}.$

(2) Suppose only one H_q is invariant in the whole G_{8q^2}. We may now write the relations

$$A^{-1}T_1A = T_1^a, \qquad B^{-1}T_1B = T_1^b, \qquad A^{-1}T_2A = T_2^\alpha, \qquad B^{-1}T_2B = T_1^\beta T_2^\gamma.$$

As in the preceding case $a^2 \equiv 1$. Also

$$B^{-1}A^{-1}T_1T_2AB = T_1^{ab+\alpha\beta}T_2^{\alpha\gamma}$$

and

$$A^{-3}B^{-1}T_1T_2BA^3 = T_1^{a^3b+\alpha^3b}T_2^{\alpha^3\gamma}.$$

Hence $\beta \equiv 0$ or $a \equiv \alpha$ and, therefore this case is impossible.

(3) Suppose no H_q is invariant in our G_{8q^2}.

(a) If there is one H_q and, therefore, two H_q invariant under A we have

$$A^{-1}T_1A = T_1^a, \qquad B^{-1}T_1B = T_1^bT_2^c$$

$$A^{-1}T_2A = T_2^a, \qquad B^{-1}T_2B = T_1^\beta T_2^\gamma.$$

Transforming $$B^{-1}A^{-1}T_1^xT_2^yAB = T_1^{abx+a\beta y}T_2^{acx+a\gamma y}$$

and $$A^{-3}B^{-1}T_1^xT_2^yBA^3 = T_1^{a^3bx+a^3\beta y}T_2^{a^3cx+a^3\gamma y}.$$

Hence we get the four congruences:

$$ab \equiv a^3b, \qquad a\beta \equiv a^3\beta, \qquad ac \equiv a^3c, \qquad a\gamma \equiv a^3\gamma.$$

If $b \not\equiv 0$, then $a^2 \equiv 1$; and since $\beta \not\equiv 0$, we have $a \equiv \alpha$. But if $a \equiv \alpha$ all the H_q are invariant under A and since $2H_q$ are invariant under B we have case (1). Hence we must assume $b \equiv 0$. Likewise we must have $\gamma \equiv 0$. It is also seen that $\alpha \equiv a^3$ and $a \equiv \alpha^3$, a and α belonging to the exponent 4 (mod q). Let us now put T_2' in place of T_2^c and keep T_1 fixed. Therefore

$$B^{-1}T_1B = T_2'$$

and $$B^{-1}T_2'B = B^{-1}T_2^cB = T_1^{\beta c}.$$

But $$T_1 = B^{-2}T_1B^2 = B^{-1}T_2^cB = T_1^{\beta c}$$

whence $$\beta c \equiv 1 \pmod q.$$

Hence, dropping primes, we may write our relations:

$$A^{-1}T_1A = T_1^a, \qquad B^{-1}T_1B = T_2, \qquad A^{-1}T_2A = T_2^a, \qquad B^{-1}T_2B = T_1.$$

No matter how we transform or change our generators no inconsistency in these relations arises, and hence we get a single type of G_{8q^2}.

(b) If no H_q is invariant under A, proceeding as in § 3 for the corresponding case, we have the relations;

$$A^{-1}T_1A = T_2, \qquad B^{-1}T_1B = T_1^a, \qquad A^{-1}T_2A = T_1^{-1}, \qquad B^{-1}T_2B = T_1^\alpha T_2^\beta.$$

Therefore $$B^{-1}A^{-1}T_1AB = B^{-1}T_2B = T_1^\alpha T_2^\beta$$

and $$A^{-3}B^{-1}T_1BA^3 = A^{-3}T_1^aA^3 = T_2^{-a}.$$

Hence we have $\alpha \equiv 0$ and $\beta \equiv -a$. This gives but a single type of G_{8q^2}, for $a \equiv +1$, $\beta \equiv -1$ and $a \equiv -1$, $\beta \equiv +1$ merely amount to an interchange of T_1 and T_2.

11. $H_{p^3} = \{ A^4 = 1,\ B^2 = A^2,\ B^{-1}AB = A^3 \}$.

(i) Suppose there are qH_8. In this case the H_{q^2} are non-cyclic. Our relations may now be written in the form

(1) $A^{-1}T_1A = T_1, \quad B^{-1}T_1B = T_1, \quad A^{-1}T_2A = T_2^a, \quad B^{-1}T_2B = T_1^\beta T_2^b.$

Transforming

(2) $B^{-1}A^{-1}T_2AB = T_1^{a\beta}T_2^{ab}$ and $A^{-3}B^{-1}T_2BA^3 = T_1^\beta T_2^{a^3b}$.

Since $AB = BA^3$ we see that $\beta \equiv 0$ or $a \equiv 1$, and hence in either case we may write, assuming $\beta \equiv 0$,

$$A^{-1}T_2A = T_2^a, \qquad B^{-1}T_2B = T_2^b.$$

Therefore

$$A^{-2}T_2A^2 = T_2^{a^2}, \qquad B^{-2}T_2B^2 = T_2^{b^2}.$$

Hence $a^2 \equiv b^2$ and since $b \not\equiv 0$, we have $a^2 \equiv 1$ from (2). If $a, b \equiv -1$, by taking AB in place of A we find that T_2 is transformed into itself; while if $a \equiv -1$, $b \equiv +1$, by taking A^2B in place of A, T_2 is transformed into itself. Hence, in each case, we can assume $a \equiv +1$ and then the only value b can have is -1. It follows, then, that relations (1) give only one type which is the direct product of $\{T_1\}$ and $\{T_2, A, B\}$.

(ii) q^2H_8. For the *cyclic* H_{q^2} we get, just as in the preceding case, one type with the relations:

$$A^{-1}TA = T^a, \qquad B^{-1}TB = T^b$$

where $a \equiv +1$ and $b \equiv -1 \pmod{q^2}$.

Non-cyclic H_{q^2}.

(1) Suppose the H_{q^2} contains $2H_q$ invariant in our G_{8q^2}. Therefore

$$A^{-1}T_1A = T_1^a, \quad B^{-1}T_1B = T_1^b, \quad A^{-1}T_2A = T_2^\alpha, \quad B^{-1}T_2B = T_2^\beta.$$

As in (i) we can assume $a \equiv +1$, $b \equiv -1 \pmod q$. We cannot have α and β both congruent to $+1$. This gives one type of G_{8q^2} with the relations

$$A^{-1}T_1A = T_1, \quad B^{-1}T_1B = T_1^{-1}, \quad A^{-1}T_2A = T_2, \quad B^{-1}T_2B = T_2^{-1}.$$

Only one other type of G_{8q^2} is possible, for if we have

$$A^{-1}T_1A = T_1, \quad B^{-1}T_1B = T_1^{-1}, \quad A^{-1}T_2A = T_2^{-1}, \quad B^{-1}T_2B = T_2^{-1},$$

then by keeping A fixed and replacing B by AB we have

$$A^{-1}T_1A = T_1, \quad B^{-1}T_1B = T_1^{-1}, \quad A^{-1}T_2A = T_2^{-1}, \quad B^{-1}T_2B = T_2.$$

(2) The case of only one H_q invariant in the whole G_{8q^2} may be shown impossible just as in § 10.

5. Suppose there is no H_q invariant in the whole G_{8q^2}, but let there be one H_q commutative with A. Our relations may now be written

$$A^{-1}T_1A=T_1^a, \qquad B^{-1}T_1B=T_1^bT_2^c, \qquad A^{-1}T_2A=T_2^\alpha, \qquad B^{-1}T_2B=T_1^\beta T_2^\gamma.$$

Transforming $$A^{-1}B^{-1}T_1^xT_2^yBA=T_1^{abx+a\beta y}\,T_2^{\alpha cx+\alpha\gamma y},$$

and $$B^{-1}A^{-1}T_1^xT_2^yAB=T_1^{abx+\alpha\beta y}\,T_2^{acx+\alpha\gamma y}.$$

Hence we have the congruences:

$$(1)\ ab\equiv \alpha^2 b, \qquad (2)\ a\beta\equiv\alpha^2\beta,$$

$$(3)\ ac\equiv\alpha^3 c, \qquad (4)\ \alpha\gamma\equiv\alpha^3\gamma.$$

Also we get by transformation

$$B^{-2}T_1B^2=T_1^{b^2+\beta c}\,T_2^{bc+\gamma c}=A^{-2}T_1A^2=T_1^{a^2},$$

and

$$B^{-2}T_2B^2=T_1^{\beta b+\beta\gamma}\,T_2^{c\beta+\gamma^2}=A^{-2}T_2A^2=T_2^{\alpha^2}.$$

Therefore we have the congruences:

$$(5)\ b^2+\beta c\equiv a^2, \qquad (6)\ bc+\gamma c\equiv 0,$$

$$(7)\ \beta b+\beta\gamma\equiv 0, \qquad (8)\ c\beta+\gamma^2\equiv\alpha^2.$$

We must now investigate these eight congruences to determine the values of the exponents $a, b, c, \alpha, \beta, \gamma$. It may be noted that $c, \beta \not\equiv 0$ for otherwise we have a preceding case. From (7) if $b\equiv 0$ then $\gamma\equiv 0$, and if $b\not\equiv 0$ then $\gamma\not\equiv 0$, also $b^2\equiv\gamma^2$ and hence from (5) and (8) $a^2\equiv\alpha^2$.

First, suppose $\qquad b\not\equiv 0.$

From (1) $\qquad \alpha^2\equiv 1$

and since by (2) $\qquad a\equiv\alpha^3$

we have $\qquad \alpha\equiv a.$

We may now have two cases.

(i) B is permutable with one H_q and, therefore, with two H_q. This is clearly the same as case (1) since $2H_q$ are invariant in G_{8q^2}.

(ii) B is permutable with no H_q. Now

$$B^{-1}T_1^xT_2^yB=T_1^{bx+\beta y}T_2^{cx+\gamma y}\equiv T_1^{bx+\beta y}T_2^{cx-by}$$

by (7). Taking σ as a Galoisian imaginary we have

$$B^{-1}T_1^xT_2^yB=(T_1^xT_2^y)^\sigma.$$

Hence we must have the congruences

$$bx + \beta y \equiv \sigma x,$$

$$cx + by \equiv \sigma y.$$

Eliminating x and y we have

$$\sigma \equiv c\beta + b^2 \equiv a^2 \quad \text{by (5)}.$$

Hence $\sigma^2 \equiv 1$, so that σ is real, contrary to hypothesis.

Secondly, suppose $b \equiv 0$. Since $b, \gamma \equiv 0$ we have

$$A^{-1}T_1A = T_1^a, \qquad B^{-1}T_1B = T_2^c, \qquad A^{-1}T_2A = T_2^a, \qquad B^{-1}T_2B = T_1^\beta.$$

Let $T_2' = T_2^c$ and then our invariant $H_{q^2} = \{T_1, T_2'\}$. Hence

$$B^{-1}T_2'B = B^{-1}T_2^cB = T_1^{\beta c} = T_1^{a^2}$$

from (5).

(*a*) $a^2 \equiv +1$. Here $a \equiv \alpha$ from (2) so that dropping primes we have

$$A^{-1}T_1A = T_1^a, \qquad B^{-1}T_1B = T_2, \qquad A^{-1}T_2A = T_2^a, \qquad B^{-1}T_2B = T_1.$$

These relations show that $\{T_1T_2\}$ is invariant in G_{8q^2}, contrary to hypothesis.

(*b*) $a^2 \equiv -1$. From (2) $\alpha \equiv -a$ so that we have the relations

$$A^{-1}T_1A = T_1^a, \qquad B^{-1}T_1B = T_2, \qquad A^{-1}T_2A = T_2^{a^3}, \qquad B^{-1}T_2B = T_1^{-1},$$

which furnish a single type of G_{8q^2}.

(4) Suppose no non-identical element of $\{A, B\}$ is commutative with an H_q. Then each non-identical element of $\{A\}$ and of $\{B\}$ corresponds to a non-identical isomorphism of H_{q^2}. According to § 7 the substitutions or isomorphisms of H_{q^2} with irreducible congruences divide into groups J forming a single conjugate set. Since $\{A\}$ and $\{B\}$ are not conjugate the corresponding groups of substitutions are not conjugate, and thus we have a contradiction. Accordingly there is no type of G_{8q^2} in the present case. As regards the correspondence between the elements of $\{A, B\}$ and the isomorphisms J, see HÖLDER, Mathematische Annalen, Vol. 43, p. 329.

12. $\qquad H_{p^3} = \{A^{p^2} = B^p = 1, \qquad B^{-1}AB = A^{p+1}\}$ (p odd)

(i) qH_{p^3}. Since the H_{q^2} must be non-cyclic we have the relations;

(*a*) $A^{-1}T_1A = T_1, \quad B^{-1}T_1B = T_1, \quad A^{-1}T_2A = T_2^a, \quad B^{-1}T_2B = T_2^b,$

for if we have $B^{-1}T_2B = T_1^cT_2^b$ instead of the last relation above, then

$$B^{-1}A^{-1}T_1T_2AB = T_1^{1+ac}T_2^{ab}$$

and

$$A^{-p-1}B^{-1}T_1T_2BA^{p+1} = T_1^{1+c}T_2^{a^{p+1}b},$$

Therefore $c \equiv 0$ or $a \equiv 1$ and hence in either case we have relations of the form (a). From the above transformation we have

$$a^p \equiv 1 \pmod{q}.$$

If $a, b \not\equiv 1 \pmod{q}$ we can choose an integer k such that $ab^k \equiv 1$, and if we take AB^k as a generator in place of A, keeping B fixed, T_2 is transformed into itself. Hence we may assume $a \equiv 1$ and our relations become

$$A^{-1}T_1A = T_1, \qquad B^{-1}T_1B = T_1, \qquad A^{-1}T_2A = T_2, \qquad B^{-1}T_2B = T_2^b.$$

where b belongs to the exponent $p \pmod{q}$. Any $G_{p^3q^2}$ formed from these relations is the direct product of $\{T_1\}$ and $\{T_2, A, B\}$. WESTERN (l. c., p. 223) shows that there are $p-1$ types of $\{T_2, A, B\}$ corresponding to the $p-1$ primitive roots of

$$a^p \equiv 1 \pmod{q}.$$

Hence we have $p-1$ types of $G_{p^3q^2}$.

If $b \equiv 1$, $a \not\equiv 1$ in relations (a) then a belongs to the exponent $p \pmod{q}$ and we get one type of $G_{p^3q^2}$, for taking A^x in place of A all our relations are unaltered, except that a is replaced by a^x.

(ii) Let there be $q^2 H_{p^3}$ and also $q \equiv 1 \pmod{p}$. For *cyclic* H_{q^2} our relations may be written

$$A^{-1}TA = T^a, \qquad B^{-1}TB = T^b.$$

If $a \equiv 1$ and b belongs to the exponent $p \pmod{q^2}$, just as in (i) we get $p-1$ types corresponding to the $p-1$ primitive roots of

$$b^p \equiv 1 \pmod{q^2}.$$

The same $p-1$ types will be obtained if both a and b belong to the exponent $p \pmod{q^2}$. If $b \equiv 1$ and a belongs to the exponent $p \pmod{q^2}$ we have one type. Just as in (i) it may be shown that a cannot belong to the exponent $p^2 \pmod{q^2}$.

Non-cyclic H_{q^2}.

(1) Suppose $2H_q$ are invariant in the whole $G_{p^3q^2}$. Our relations may now be written

$$A^{-1}T_1A = T_1^a, \qquad B^{-1}T_1B = T_1^b, \qquad A^{-1}T_2A = T_2^\alpha, \qquad B^{-1}T_2B = T_2^\beta.$$

Neither a nor α can belong to the exponent $p^2 \pmod{q}$. If $a, b \not\equiv 1$ we can change generators, as above in (i), so as to make $a \equiv 1$. Hence we have two cases:

(I) $a \equiv 1 \pmod{q}$ b belonging to exponent $p \pmod{q}$.

(II) $b \equiv 1 \pmod{q}$ a belonging to exponent $p \pmod{q}$.

If in (I) $\alpha \equiv 1$, we have the relations:

$$A^{-1}T_1A = T_1, \qquad B^{-1}T_1B = T_1^b, \qquad A^{-1}T_2A = T_2, \qquad B^{-1}T_2B = T_2^\beta.$$

Since different primitive roots b, β furnish different types, we have here $(p-1)^2$ types of $G_{p^3q^2}$. Again, if in (I) $\alpha \not\equiv 1$, $\beta \equiv 1$ we have $p-1$ types with the relations:

$$A^{-1}T_1A = T_1, \qquad B^{-1}T_1B = T_1^b, \qquad A^{-1}T_2A = T_2^{\alpha}, \qquad B^{-1}T_2B = T_2.$$

In case (I) if α, $\beta \not\equiv 1$ we have $(p-1)^2$ types with the relations:

$$A^{-1}T_1A = T_1, \qquad B^{-1}T_1B = T_1^b, \qquad A^{-1}T_2A = T_2^{\alpha}, \qquad B^{-1}T_2B = T_2^{\beta}.$$

In case (II) there are $\frac{1}{2}(p+1)$ types [cf. § 6 (ii) (2)] with the relations:

$$A^{-1}T_1A = T_1^{a}, \qquad B^{-1}T_1B = T_1, \qquad A^{-1}T_2A = T_2^{a}, \qquad B^{-1}T_2B = T_2.$$

The case in which a, α, β all belong to the exponent $p \pmod{q}$ easily reduces to a preceding case.

(2) Suppose there is only one H_q invariant in the whole $G_{p^3q^2}$. Our relations may now be written

$$A^{-1}T_1A = T_1^{a}, \qquad B^{-1}T_1B = T_1^b, \qquad A^{-1}T_2A = T_2^{\alpha}, \qquad B^{-1}T_2B = T_1^{\beta}T_2^{\gamma}.$$

As in the preceding discussion we may assume that a belongs to the exponent $p \pmod{q}$. By transformation

$$B^{-1}A^{-1}T_1T_2AB = T_1^{ab+\alpha\beta}T_2^{\alpha\gamma}, \qquad A^{-(p+1)}B^{-1}T_1T_2BA^{p+1} = T_1^{ab+a\beta}T_2^{\alpha\gamma}.$$

Hence $$\alpha\beta \equiv a\beta.$$

If $\beta \equiv 0$ we have two H_q invariant in $G_{p^3q^2}$. Hence $\beta \not\equiv 0$ and therefore $a \equiv \alpha$. It follows, then, that all the H_q are invariant under A and hence we may pick out our generators so that two H_q are invariant in the whole group, contrary to hypothesis.

(3) Suppose there is no H_q invariant in the $G_{p^3q^2}$. Since there will always be two H_q invariant under A, our relations may be written

$$A^{-1}T_1A = T_1^{a}, \qquad B^{-1}T_1B = T_1^bT_2^c, \qquad A^{-1}T_2A = T_2^{\alpha}, \qquad B^{-1}T_2B = T_1^{\beta}T_2^{\gamma}.$$

By transformation $\quad B^{-1}A^{-1}T_1^xT_2^yAB = T_1^{abx+\alpha\beta y}T_2^{acx+\alpha\gamma y}$

and $$A^{-(p+1)}B^{-1}T_1^xT_2^yBA^{p+1} = T_1^{a^{p+1}bx+a^{p+1}\beta y}T_2^{\alpha^{p+1}cx+\alpha^{p+1}\gamma y}.$$

We must have c, $\beta \not\equiv 0$ and hence, comparing exponents,

$$\alpha \equiv a^{p+1} \quad \text{and} \quad a \equiv \alpha^{p+1}.$$

Hence $$\alpha \equiv a^{p+1} \equiv (\alpha^{p+1})^{p+1} \equiv \alpha^{p^2+2p+1} \equiv \alpha^{2p+1}.$$

Whence $$\alpha^{2p} \equiv 1$$

and therefore $$\alpha^p \equiv \pm 1.$$

Since p is odd we cannot have $\alpha^p \equiv -1$ so that

$$\alpha^p \equiv 1 \equiv a^p.$$

Hence $a \equiv \alpha$ and since all the H_q are invariant under A and two H_q are invariant under B, two H_q are invariant in the whole group, contrary to hypothesis.

13. *$q^2H_{p^3}$ and $q \equiv -1 \pmod p$.* No element of order q can be transformed by A or B into a power of itself different from unity. Let us consider the relations:

(1) $A^{-1}T_1A = T_2, \quad B^{-1}T_1B = T_1, \quad A^{-1}T_2A = T_1^{-1}T_2^b, \quad B^{-1}T_2B = T_2.$

Since $$B = T_1^{-1}BT_1$$

then $$A^{-1}BA = A^{-1}T_1^{-1}BT_1A,$$

and since $$A^{-1}BA = BA^{-p}$$

we have $$BA^{-p} = T_2^{-1}BA^{-p}T_2.$$

Therefore $$A^{-p} = T_2^{-1}A^{-p}T_2.$$

Again $$A^{-p}(A^{-1}T_2A)A^p = A^{-p}(T_1^{-1}T_2^b)A^p.$$

Hence $$T_1^{-1}T_2^b = A^{-p}T_1^{-1}A^pT_2^b$$

and $$T_1^{-1} = A^{-p}T_1^{-1}A^p.$$

It follows then that A^p and T_1, T_2, are commutative. Hence relations (1) furnish but a single type of $G_{p^3q^2}$, where b is determined by Galoisian imaginaries as in § 3 (ii).

Next we will consider the relations

(2) $A^{-1}T_1A = T_1, \quad B^{-1}T_1B = T_2, \quad A^{-1}T_2A = T_2, \quad B^{-1}T_2B = T_1^{-1}T_2^b.$

The relation $B^{-1}T_1B = T_2$ can be written $B^{-1}T_1B = T_1^i$ where i is a Galoisian imaginary and a primitive root of the congruence

$$i^p \equiv 1 \pmod q.$$

Different primitive roots of this congruence give different types of groups (cf. WESTERN, l. c., p. 223). Hence relations (2) give $p-1$ types of $G_{p^3q^2}$.

There is no further type, for the supposition that no element of $\{A, B\}$ is commutative with an H_q is inadmissible, just as in § 11 for the corresponding case.

14. $H_{p^3} = \{A^p = B^p = C^p = 1,\ AB = BA,\ AC = CA,\ B^{-1}CB = A^{-1}C\}$ (p odd).

(i) Suppose there are qH_{p^3}. Hence

$$q \equiv 1 \pmod p.$$

Since the H_{q^2} is non-cyclic our relations may be written in the form

$$(1)\qquad \begin{array}{lll} A^{-1}T_1A = T_1, & B^{-1}T_1B = T_1, & C^{-1}T_1C = T_1, \\ A^{-1}T_2A = T_2^a, & B^{-1}T_2B = T_1^\beta T_2^b, & C^{-1}T_2C = T_1^\gamma T_2^c, \end{array}$$

Now
$$B^{-1}A^{-1}T_1T_2AB = T_1^{1+a\beta}T_2^{ab}$$
and
$$A^{-1}B^{-1}T_1T_2BA = T_1^{1+\beta}T_2^{ab}.$$

Hence $\beta \equiv 0$ or $a \equiv 1$, and therefore we may assume $\beta \equiv 0$ in (1). Also

$$C^{-1}B^{-1}T_1T_2BC = C^{-1}T_1T_2^bC = T_1^{1+\gamma b}T_2^{cb}$$

and
$$B^{-1}A^{-1}C^{-1}T_1T_2CAB = B^{-1}A^{-1}T_1^{1+\gamma}T_2AB = T_1^{1+\gamma}T_2^{abc}.$$

Since $BC = CAB$ we have the congruences:

$$1 + \gamma b \equiv 1 + \gamma \qquad \text{and} \qquad cb \equiv abc.$$

Now $c \not\equiv 0$ for otherwise T_2 would be independent of T_1. Hence $a \equiv 1$.
From
$$\gamma b \equiv \gamma \qquad \text{either} \qquad \gamma \equiv 0 \qquad \text{or} \qquad b \equiv 1.$$

In the latter case all the H_q are permutable with A and B and since $2H_q$ are permutable with C we may assume $\gamma \equiv 0$, and hence we have the relations:

$$(2)\qquad \begin{array}{lll} A^{-1}T_1A = T_1, & B^{-1}T_1B = T_1, & C^{-1}T_1C = T_1, \\ A^{-1}T_2A = T_2, & B^{-1}T_2B = T_2^b, & C^{-1}T_2C = T_2^c. \end{array}$$

If $b,\ c \not\equiv 1$ we can set $b \equiv c^x$ and now in place of B let us take BC^k. Hence

$$C^{-k}B^{-1}T_2BC^k = T_2^{c^{x+k}}.$$

If, then, k is so chosen that $x + k \equiv 0$, T_2 is transformed into itself, and accordingly we can assume $b \equiv 1$ in relations (2). We thus get a single type of $G_{p^3q^2}$ which is the direct product of $\{T_1\}$ and $\{B,\ C,\ A,\ T_2\}$.

(ii) Suppose there are $q^2H_{p^3}$ with $q \equiv 1 \pmod p$. As in the preceding discussion we may write our relations for the *cyclic* H_{q^2}.

$$A^{-1}TA = T, \qquad B^{-1}TB = T, \qquad C^{-1}TC = T^c.$$

This gives us a single type of $G_{p^3q^2}$, c belonging to the exponent $p \pmod{q^2}$.

For *non-cyclic* H_{q^2} we have different cases:

(1) Suppose two H_q, $\{T_1\}$, $\{T_2\}$ are invariant in the whole $G_{p^3q^2}$. Hence

$$(a)\qquad \begin{aligned} A^{-1}TA &= T_1^a, & B^{-1}T_1B &= T_1^b, & C^{-1}T_1C &= T_1^c, \\ A^{-1}T_2A &= T_2^a, & B^{-1}T_2B &= T_2^\beta, & C^{-1}T_2C &= T_2^\gamma. \end{aligned}$$

As in the preceding we may assume $a \equiv \alpha \equiv 1 \pmod q$. We may then choose our elements so as to make $b \equiv 1$ or $c \equiv 1$. Let us say that

$$b \equiv 1,$$

then if $\beta, \gamma \not\equiv 1$ we may let $\gamma \equiv \beta^y$ and keeping B fixed, put B^kC in place of C. Therefore $C^{-1}B^{-k}T_2B^kC = T_2^{\beta^{k+y}}$.

Now let k be so chosen that $k + y \equiv 0$. Hence we have the relations

$$\begin{aligned} A^{-1}T_1A &= T_1, & B^{-1}T_1B &= T_1, & C^{-1}T_1C &= T_1^c, \\ A^{-1}T_2A &= T_2, & B^{-1}T_2B &= T_2^\beta, & C^{-1}T_2C &= T_2. \end{aligned}$$

We, thus, have a single type of $G_{p^3q^2}$; for if we take $B_0 = B^y$, $C_0 = C^x$, $A_0 = A^{xy}$ the relations for our H_{p^3} are unaltered. c and β belong to the exponent p $(\bmod q)$.

If in relations (a) $\beta \equiv 1$ we get $(p+1)/2$ types with the relations

$$\begin{aligned} A^{-1}T_1A &= T_1, & B^{-1}T_1B &= T_1, & C^{-1}T_1C &= T_1^c, \\ A^{-1}T_1A &= T_2, & B^{-1}T_2B &= T_2, & C^{-1}T_2C &= T_2^\gamma. \end{aligned}$$

(2) Suppose only one H_q invariant in the whole $G_{p^3q^2}$. After a proper change of generators our relations may be written

$$\begin{aligned} A^{-1}T_1A &= T_1, & B^{-1}T_1B &= T_1\quad, & C^{-1}T_1C &= T_1^c\quad, \\ A^{-1}T_2A &= T_2^a, & B^{-1}T_2B &= T_1^\beta T_2^\lambda, & C^{-1}T_2C &= T_1^\gamma T_2^\mu. \end{aligned}$$

Hence $$C^{-1}B^{-1}T_1T_2BC = T_1^{c+c\beta+\lambda\gamma}T_2^{\lambda\mu},$$

and $$B^{-1}A^{-1}C^{-1}T_1T_2CAB = T_1^{c+\gamma+a\beta\mu}T_2^{a\lambda\mu}.$$

Since $$\lambda,\ \mu \not\equiv 0 \text{ we have } a \equiv 1.$$

Consequently by a proper change of generators, we may assume $\beta \equiv 0$. Hence $\lambda\gamma \equiv \gamma$ and, since

$$\gamma \not\equiv 0,$$

we have $$\lambda \equiv 1.$$

This makes all the H_q invariant under A and B and, since two are invariant under C, two H_q will be invariant in the whole $G_{p^3q^2}$, contrary to hypothesis.

(3) Suppose there is no H_q invariant in the whole $G_{p^3q^2}$. Since $q \equiv 1 \pmod{p}$ and p is odd two H_q, at least, are permutable with A or B or C. In $\{A, B, T_1, T_2\}$ two H_q are invariant under both A and B [cf. § 6 (ii)]. Hence we have the relations

$$A^{-1}T_1A = T_1^a, \qquad B^{-1}T_1B = T_1^b, \qquad C^{-1}T_1C = T_1^cT_2^d,$$

$$A^{-1}T_2A = T_2^\alpha, \qquad B^{-1}T_2B = T_2^\beta, \qquad C^{-1}T_2C = T_1^\gamma T_2^\delta.$$

Now
$$C^{-1}A^{-1}T_1T_2AC = T_1^{ac+\alpha\gamma}T_2^{ad+\alpha\delta}$$

and
$$A^{-1}C^{-1}T_1T_2CA = T_1^{ac+a\gamma}T_2^{ad+a\delta}.$$

Since
$$\gamma \not\equiv 0 \quad \text{we have} \quad a \equiv \alpha.$$

Also
$$C^{-1}B^{-1}T_1^xT_2^yBC = T_1^{cbx+\beta\gamma y}T_2^{dbx+\delta\beta y}$$

and
$$B^{-1}A^{-1}C^{-1}T_1^xT_2^yCAB = T_1^{abcx+ab\gamma y}T_2^{a\beta dx+a\beta\delta y}.$$

Hence we have the four congruences:

(1) $cb \equiv abc$, (2) $\beta\gamma \equiv ab\gamma$, (3) $db \equiv a\beta d$, (4) $\delta\beta \equiv a\beta\delta$.

From (2) we see that if $a \equiv 1$ then $\beta \equiv b$, and hence there would be two H_q invariant in the whole $G_{p^3q^2}$. Therefore we must have $a, \alpha \not\equiv 1$. Keeping A and C fixed and taking A^kB in place of B we can assume $b \equiv 1$, provided k is properly chosen.

From (2) $\gamma\beta \equiv ab\gamma \equiv a\gamma$ and since $\gamma \not\equiv 0$, $\beta \equiv a$.

From (4) $\beta\delta \equiv a\beta\delta \equiv \beta^2\delta$, and since

$$\beta \not\equiv 1 \qquad \text{then} \qquad \delta \equiv 0.$$

Hence from (3)
$$d \equiv a\beta d \equiv a^2d.$$

Since
$$d \not\equiv 0, \qquad a^2 \equiv 1,$$

and hence
$$a \equiv -1 \equiv \beta.$$

Since p is odd B may be replaced by B^2, so that B transforms both T_1 and T_2 into themselves. Hence there are two H_q invariant in the whole $G_{p^3q^2}$, contrary to hypothesis.

15. *$q^2H_{p^3}$ and $q \equiv -1 \pmod{p}$.* Here the H_{q^2} must be non-cyclic. Neither T_1 nor T_2 can be transformed into any of its powers, except the first, by A, B or C.

The set of relations:

$$A^{-1}T_1A = T_2, \qquad B^{-1}T_1B = T_1, \qquad C^{-1}T_1C = T_1,$$

$$A^{-1}T_2A = T_1^{-1}T_2^b, \qquad B^{-1}T_2B = T_2, \qquad C^{-1}T_2C = T_2,$$

do not furnish a type, for

$$C^{-1}B^{-1}T_1BC=T_1 \qquad \text{and} \qquad B^{-1}A^{-1}C^{-1}T_1CAB=T_2,$$

whence it follows that $T_1=T_2$.

If A transforms as above, neither B nor C can transform T_1 and T_2 in a different way from that above {cf. § 11 (4)}. Hence if a type exists in our supposed case A must be permutable with T_1 and T_2, and then so far as the matter of isomorphism is concerned $BC=CB$, since A corresponds to the identical isomorphism. The only type then, that we can have, has the relations {cf. § 11 (4)}

$$A^{-1}T_1A=T_1, \qquad B^{-1}T_1B=T_2, \qquad C^{-1}T_1C=T_1,$$
$$A^{-1}T_2A=T_2, \qquad B^{-1}T_2B=T_1^{-1}T_2^b, \qquad C^{-1}T_2C=T_2.$$

III.

$G_{p^3q^2}$ HAVING AN INVARIANT H_{p^3} AND MORE THAN ONE H_{q^2}.

16. *General considerations.* If the elements of H_{p^3} are all transformed by T, T_1, or T_2, we get the same elements in different order. Each element of an H_{q^2} corresponds to an isomorphism of H_{p^3}. It follows, then, that q must be a divisor of the order of the group of isomorphisms of H_{p^3}. The orders of the groups of isomorphisms for the various types of H_{p^3} are given by WESTERN, l. c., pp. 211–216.

If $G_{p^3q^2}$ contains pH_{q^2} then the H_{p^3} must contain an H_{p^2} *each element* of which is commutative with an H_{q^2}.

If $G_{p^3q^2}$ contains $p^2H_{q^2}$ then the H_{p^3} must contain an H_p *each element* of which is commutative with an H_{q^2}.

If S represents one of the elements of H_{p^3} commutative with an H_{q^2} mentioned above then

$$S^{-1}TS=T^k$$

and hence

$$S^{-1}(TST^{-1})=T^{k-1}.$$

Since our H_{p^3} is invariant TST^{-1} is an element of H_{p^3} and, therefore, T^{k-1} is also.

Hence

$$k\equiv 1 \pmod{q^2}$$

thus making S and T commutative.

If the H_{q^2} are non-cyclic then we must consider two cases:

(i) $$S^{-1}T_1S=T_1^a, \qquad S^{-1}T_2S=T_2^b,$$

(ii) $$S^{-1}T_1S=T_2, \qquad S^{-1}T_2S=T_1^\alpha T_2^\beta,$$

In case (i)

$$S^{-1}(T_1ST_1^{-1})=T_1^{a-1} \qquad \text{and} \qquad S^{-1}(T_2ST_1^{-1})=T_2^{b-1}.$$

Now just as in the above cyclic case

$$a \equiv b \equiv 1 \pmod q.$$

Hence T_1, T_2 and S are all commutative. In case (ii)

$$S^{-1}(T_1 S T_1^{-1}) = T_2 T_1^{-1}, \qquad \text{and} \qquad S^{-1}(T_2 S T_2^{-1}) = T^{\alpha} T_2^{\beta-1}.$$

Therefore $T_2 T_1^{-1}$ belongs to H_{p^3} which is impossible. Hence case (ii) is excluded.

In considering each type of H_{p^3} we will divide into cases according to the number of H_{q^2} contained in $G_{p^3q^2}$.

17. *H_{p^3} cyclic, say* $A^{p^3} = 1$. The order of the group of isomorphisms is $p^2(p-1)$, and hence

$$p \equiv 1 \pmod q.$$

pH_{q^2}. The H_{p^2}, each of whose elements is permutable with the elements of an H_{q^2}, must be $\{A^p\}$. Hence

$$A^{-p} T A^p = T,$$

and since $\{A\}$ is invariant in the $G_{p^3q^2}$

$$T^{-1} A T = A^{\alpha}.$$

This leads to two cases, according as α belongs to the exponent q or q^2 mod p^3.

Now $$T^{-1} A^p T = A^{\alpha p} = A^p.$$

Hence $$\alpha = 1 + kp^2.$$

Therefore $$\alpha^q = (1 + kp^2)^q \equiv 1 + kqp^2 \pmod{p^3} \equiv 1 \pmod{p^3},$$

or $$\alpha^{q^2} = (1 + kp^2)^{q^2} \equiv 1 + kq^2p^2 \pmod{p^3} \equiv 1 \pmod{p^3}.$$

In either case $k \equiv 0 \pmod p$ and hence A and T are permutable, contrary to hypothesis. We evidently obtain the same result if the H_{q^2} are non-cyclic.

$p^2H_{q^2}$. Proceeding in the same way as above we find that no type of $G_{p^3q^2}$ exists in our supposed case.

$p^3H_{q^2}$. For cyclic H_{q^2} we have

$$T^{-1} A T = A^{\alpha}.$$

We get two types of $G_{p^3q^2}$ according as α belongs to the exponent q or q^2 $\pmod{p^3}$.

For non-cyclic H_{q^2} we have the relations

$$T_1^{-1} A T_1 = A^{\alpha}, \qquad T_2^{-1} A T_2 = A^{b},$$

as in preceding work we may assume one of the exponents, say $b \equiv 1$, while α belongs to the exponent q mod p^3. Hence we get one type of $G_{p^3q^2}$ which is the direct product of an H_{p^3q} and an H_q.

18. $H_{p^3} = [A^{p^2} = B^p = 1, AB = BA]$. The order of the group of isomorphisms is $p^3(p-1)^2$. Hence $p \equiv 1 \pmod q$.

pH_{q^2}. The H_{p^2} with whose elements those of an H_{q^2} are commutative is either $\{A^p, B\}$ or $\{A\}$, where $\{A\}$ is typical of the pH_{p^2} $\{AB^\kappa\}$ $(\kappa \equiv 0, 1, 2, \cdots, p-1)$. If we take the former case, then

(1) $$A^{-p}TA^p = T, \qquad B^{-1}TB = T.$$

Since there are p cyclic H_{p^2} in H_{p^3} one at least is permutable with T. Suppose this is $\{A\}$. Then

(2) $$T^{-1}AT = A^a$$

and, as in the preceding, there are two cases. From (1) and (2) we see that $ap \equiv p \pmod{p^2}$. Hence

$$a = 1 + kp.$$

This makes $G_{p^3q^2}$ Abelian, for

$$a^q = (1+kp)^q \equiv 1 + kqp \pmod{p^2} \equiv 1 \pmod{p^2},$$

or

$$a^{q^2} = (1+kp)^{q^2} \equiv 1 + kq^2p \pmod{p^2} \equiv 1 \pmod{p^2}.$$

Hence in either case $k \equiv 0 \pmod p$. Likewise it may be shown that no type of $G_{p^3q^2}$ exists in the case of non-cyclic H_{q^2}.

Next let us take T permutable with the elements of $\{A\}$. One at least, of the pH_p, $\{A^{kp}B\}$, $(k \equiv 0, 1, 2, \cdots, p-1)$ is permutable with T. Taking this as $\{B\}$ we have

$$T^{-1}BT = B^a.$$

We thus get two types of $G_{p^3q^2}$ according as a belongs to the exponent q or $q^2 \pmod p$. Each is the direct product of $\{A\}$ and $\{B, T\}$. Concerning the latter group, see HÖLDER, Mathematische Annalen, vol. 43, pp. 357–9).

Let us take the non-cyclic H_{q^2}, in which T_1, T_2 are permutable with A.

We may now assume the relations:

$$T_1^{-1}BT_1 = B^a, \qquad T_2^{-1}BT_2 = A^{\kappa p}B.$$

Hence $$T_2^{-1}T_1^{-1}BT_1T_2 = A^{akp}B^a = T_1^{-1}T_2^{-1}BT_2T_1 = A^{\kappa p}B^a.$$

Therefore $$akp \equiv kp \pmod{p^2}$$

and hence $$k \equiv 0 \qquad \text{or} \qquad a \equiv 1.$$

Whence it follows that in either case our relations take the form:

$$T_1^{-1}BT_1 = B^a, \qquad T_2^{-1}BT_2 = B^b.$$

Here again we may assume one of the exponents, say $b \equiv 1 \pmod p$. We thus get one type of $G_{p^3q^2}$ which is the direct product of $\{A\}$, $\{T_2\}$ and $\{B, T\}$.

19. $p^2H_{q^2}$. The H_p whose elements are permutable with the elements of an H_{q^2} is either $\{A^p\}$ or $\{B\}$. The case of A^p being permutable with the elements of an H_{q^2} may be shown impossible just as in the preceding section.

If we take
$$T^{-1}BT = B$$

then, since there are p cyclic H_{p^2}, $\{AB^k\}$, one, at least, is permutable with T. We may take this as $\{A\}$, and then

$$T^{-1}AT = A^a$$

thus giving us two types of $G_{p^3q^2}$. Each is the direct product of $\{B\}$ and $\{A, T\}$.

For the H_{q^2} non-cyclic we have the relations (cf. § 18):

$$T_1^{-1}AT_1 = A^a, \qquad T_2^{-1}AT_2 = A^b.$$

We may consider $b \equiv 1 \pmod{p^2}$, thus giving us a single type of $G_{p^3q^2}$, the direct product of $\{T_2\}$, $\{A, T_1\}$ and $\{B\}$.

20. $p^3H_{q^2}$. First take the H_{q^2} *cyclic*. One, at least, of the p cyclic H_{p^2} is commutative with T and this may be taken as $\{A\}$. Of the pH_p one, at least, is permutable with T and this may be taken as $\{B\}$. Hence we have the relations

$$T^{-1}AT = A^a, \qquad T^{-1}BT = B^b.$$

a may belong to the exponent q or exponent q^2 mod p^2. b may belong to the exponent q or exponent q^2 mod p^2. Accordingly we have four cases to consider.

$$(1) \qquad \begin{aligned} &a \text{ a primitive root of } a^q \equiv 1 \pmod{p^2}, \\ &b \text{ a primitive root of } b^q \equiv 1 \pmod{p}. \end{aligned}$$

a may be thought of as any one of the primitive roots of

$$a^q \equiv 1 \pmod{p^2},$$

and then there are $q-1$ types of $G_{p^3q^2}$ corresponding to the $q-1$ values of b.

$$(2) \qquad \begin{aligned} &a \text{ a primitive root of } a^q \equiv 1 \pmod{p^2}, \\ &b \text{ a primitive root of } b^{q^2} \equiv 1 \pmod{p}. \end{aligned}$$

On transforming with T^x [x taking $q(q-1)$ values] we get b^x in place of b and a^y [y taking $q-1$ values] in place of a. Hence considering b as any one primitive root of

$$b^{q^2} \equiv 1 \pmod{p},$$

we get $q-1$ types corresponding to the $q-1$ values of a.

(3)
$$a \text{ a primitive root of } a^{q^2} \equiv 1 \pmod{p^2},$$
$$b \text{ a primitive root of } b^{q} \equiv 1 \pmod{p}.$$

This gives $q-1$ types of $G_{p^3q^2}$ corresponding to the $q-1$ values of b.

(4)
$$a \text{ a primitive root of } a^{q^2} \equiv 1 \pmod{p^2},$$
$$b \text{ a primitive root of } b^{q^2} \equiv 1 \pmod{p}.$$

This gives $q(q-1)$ types corresponding to the $q(q-1)$ values of b.

Non-cyclic H_{q^2}. Proceeding as in the cyclic case we may assume the relations

$$T_1^{-1}AT_1 = A^a, \qquad T_1^{-1}BT_1 = B^b, \qquad T_2^{-1}AT_2 = A^lB, \qquad T_2^{-1}BT_2 = A^{sp}B^m.$$

Transforming,
$$T_2^{-1}T_1^{-1}A^xB^yT_1T_2 = A^{alx+bspy}B^{akx+bmy}$$
and
$$T_1^{-1}T_2^{-1}A^xB^yT_2T_1 = A^{alx+aspy}B^{bkx+bmy}.$$

Hence we have the congruences

(1) $psb \equiv asp \pmod{p^2}$, (2) $ak \equiv bk \pmod{p}$.

If
$$a \not\equiv b \pmod{p}$$
then
$$s \equiv 0 \quad \text{and} \quad k \equiv 0 \pmod{p}.$$
If
$$a \equiv b \pmod{p}$$
then T_1 transforms every H_{p^2} in $\{AB^k\}$ into itself, and every H_p in $\{A^{kp}B\}$ into itself. Hence our relations take the form;

$$T_1^{-1}AT_1 = A^a, \qquad T_1^{-1}BT_1 = B^b, \qquad T_2\ AT_2 = A^\alpha, \qquad T_2^{-1}BT_2 = B^\beta.$$

b and β cannot both be $\equiv 1 \pmod{p}$, for then there would not be $p^3H_{q^2}$. Likewise we cannot have both a and $\alpha \equiv 1 \pmod{p}$. If $b,\ \beta \not\equiv 1$ we can change generators so as to assume $b \equiv 1 \pmod{p}$. Our relations may now be written in the form

$$T_1^{-1}AT_1 = A^a, \qquad T_1^{-1}BT_1 = B, \qquad T_2^{-1}AT_2 = A^\alpha, \qquad T_2^{-1}BT = B^\beta.$$

If $a \equiv 1 \pmod{p^2}$ and hence $\alpha \not\equiv 1$ we get $q-1$ types of $G_{p^3q^2}$, each being the direct product of $\{T_1\}$ and $\{T_2, A, B\}$. If $\alpha \equiv 1$, $a \not\equiv 1$ we have only one type. If α, $a \not\equiv 1$ then we can keep T_1 fixed and take $T_1T_2^r$ in place of T_2, so that A is transformed into itself provided r is chosen properly.

21. $H_{p^3} = [A^p = B^p = C^p = 1, AB = BA, AC = CA, BC = CB]$. The group of isomorphisms is of order $p^3(p-1)^3(p+1)(p^2+p+1)$.

pH_{q^2}. We must have $p \equiv 1 \pmod q$. The H_{p^2} with whose elements the elements of an H_{q^2} are permutable may be taken as $\{A, B\}$.

For cyclic H_{q^2} $T^{-1}AT = A$ and $T^{-1}BT = B$. T is permutable with $(p+1)H_p$ viz. $\{A\}$ and $\{AB^k\}$. Since

$$p^2 \equiv 1 \pmod q$$

one, at least, of the p^2 remaining H_p independent of A and B, must be permutable with T. Taking this as $\{C\}$ we have

$$T^{-1}CT = C^a.$$

This gives two types, each of which is the direct product of $H_{p^2} = \{A, B\}$ and $H_{pq^2} = \{C, T\}$. The H_{pq^2} are treated by Hölder, Matematische Annalen, Vol. 43, pp. 357–9.

Non-cyclic H_{q^2}. Here T_1, T_2 are commutative with A, B. We may assume the relations

$$T_1^{-1}CT_1 = C^a, \qquad T_2^{-1}CT_2 = C^{\alpha}B^{\beta}A^{\gamma}.$$

Whence
$$T_2^{-1}T_1^{-1}CT_1T_2 = C^{a\alpha}B^{a\beta}A^{a\gamma}$$

and
$$T_1^{-1}T_2^{-1}CT_2T_1 = C^{\alpha}B^{\beta}A^{a\gamma}.$$

Hence we have $a\alpha \equiv \alpha$ and $a\beta \equiv \beta \pmod p$. If $a \not\equiv 1$ then $\alpha \equiv 0$ and $\beta \equiv 0$. If $a \equiv 1$ then T_1 transforms every H_p into itself so that in either case we can write our relations:

$$T_1^{-1}CT_1 = C^a, \qquad T_2^{-1}CT_2 = C^{\alpha}$$

and we can assume one of the exponents, say $a \equiv 1$, thus giving us one type of $G_{p^3q^2}$ which is the direct product of $\{T_1\}$ and $\{A, B, C, T_2\}$.

22. $p^2H_{q^2}$. First we consider $p \equiv 1 \pmod q$.

Cyclic H_{q^2}. The H_p with whose elements T is permutable may be taken as $\{A\}$.

If $q > 2$ then among the $p^2 + p$ other H_p there are at least two permutable with T, and these two may be taken as $\{B\}$ and $\{C\}$. Hence we have the relations:

$$T^{-1}AT = A, \qquad T^{-1}BT = B^a, \qquad T^{-1}CT = C^b.$$

We must have $a, b \not\equiv 1$ for if either were congruent to 1 $\pmod p$ there would not be $p^2H_{q^2}$. We must consider three cases. (1) a and b both primitive roots of $a_{q^2} \equiv 1 \pmod p$. This gives $\frac{1}{2}(q^2 - q + 2)$ types of $G_{p^3q^2}$ [cf. § 4 (ii) (β)]. Each is the direct product of $\{A\}$ and $\{B, C, T\}$. (2) a and b both primitive

roots of $a^q \equiv 1 \pmod p$. This gives $\frac{1}{2}(q+1)$ types [§ 4 (ii) (α)], and they are direct products as in (1). (3) Let a be a primitive root of $a^{q^2} \equiv 1 \pmod p$ and b a primitive root of $a^q \equiv 1 \pmod p$. In this case we have $q-1$ types corresponding to the $q-1$ primitive roots of $a^q \equiv 1 \pmod p$, and these are direct products as above.

Non-cyclic H_{q^2}. ($q > 2$). T_1 and T_2 are commutative with A. A similar consideration to that in § 20 shows that we may assume the relations

$$(a)\quad T_1^{-1}CT_1 = C^a, \qquad T_1^{-1}BT_1 = B^b, \qquad T_2^{-1}CT_2 = C^\alpha, \qquad T_2^{-1}BT_2 = B^\beta,$$

a and α cannot both be congruent to 1 (mod p), and likewise for b and β. We may assume one exponent, say b, congruent to 1. Then if

$$a \equiv 1, \qquad \alpha, \beta \not\equiv 1,$$

we have $\frac{1}{2}(q+1)$ types, each the direct product of $\{A\}$, $\{T\}$ and $\{C, B, T_2\}$.

If a, $\alpha \not\equiv 1$ we may keep T_1 fixed and change the second generator T_2 so that T_2 transforms C into itself. We, thus, get one type in which $b, \alpha \equiv 1$; a, β belong to the exponent $q \pmod p$.

$q = 2$ *and* H_{q^2} *cyclic.* Besides $\{A\}$ either none or at least two H_p are permutable with T. If the latter is the case, then corresponding to (1) above we have two types; one in which

$$T^{-1}CT = C^a, \qquad T^{-1}BT = B^a,$$

and a second type in which

$$T^{-1}CT = C^a, \qquad T^{-1}BT = B^{a^3}.$$

Corresponding to (2) we have the single type with

$$T^{-1}CT = C^{-1}, \qquad T^{-1}BT = B^{-1},$$

and to (3) also a single type with

$$T^{-1}CT = C^a \quad \text{or} \quad C^{a^3}, \qquad T^{-1}BT = B^{-1}.$$

If no other H_p besides $\{A\}$ is permutable with T, then it is easily seen that we must have

$$T^{-1}BT = C.$$

Hence
$$T^{-2}BT^2 = T^{-1}CT = A^aB^aC^b,$$

also
$$T^{-3}BT^3 = A^{a+ab}B^{ab}C^{a+b^2}$$

and
$$B = T^{-4}BT^4 = A^{a+ab+aa+ab^2}B^{a^2+ab^2}C^{2ab+b^3}.$$

If T^2 and B are commutative, we have

$$T^{-1}(BC)T = BC,$$

showing that the H_p, $\{BC\}$, is permutable with T contrary to hypothesis. Hence the only possibility is that T^4 is the lowest power of T permutable with B; and, therefore, we have the congruences

$$(1) \qquad a(1+b+a+b^2) \equiv 0 \pmod{p};$$

$$(2) \qquad a(a+b^2) \equiv 1 \pmod{p};$$

$$(3) \qquad b(2a+b^2) \equiv 0 \pmod{p}.$$

If $b \equiv 0$ then $\{T^2, A, B\}$ is an H_{2p^2} with an invariant H_{p^2} and having one H_p viz., $\{A\}$, invariant. Hence there is a second H_p say $\{B\}$ invariant in H_{2p^2}. Therefore we can assume $\alpha \equiv 0$ when $b \equiv 0$. Our supposed $G_{p^3q^2}$ is the direct product of $\{A\}$ and $\{B, C, T\}$. Hence we have exactly the same case as in § 4 (ii), that is, we have one type of $G_{p^3q^2}$ with

$$\alpha \equiv b \equiv 0, \qquad a \equiv -1, \qquad p = 4m+3.$$

If $b \not\equiv 0$ then $(2a+b^2) \equiv 0$ from (3), and substituting the value of b^2 in (2) we find that

$$a^2 \equiv -1,$$

and hence p is of the form $4m+1$. Therefore

$$p^2+p+1 = 3+4k.$$

If the $4kH_p$ are transformed in k cycles of $4H_p$ each, that is, in each cycle the $4H_p$ are transformed cyclically by T; then, since $3H_p$ cannot remain fixed, there is a cycle consisting of $2H_p$, i. e., some H_p say $\{B\}$ first goes into $\{C\}$ and then $\{C\}$ goes back into $\{B\}$ under transformation by T. In every case, then, there is a cycle of $2H_p$ when all the $(p^2+p+1)H_p$ are transformed by T. This means that we may assume $\alpha \equiv 0$ and $b \equiv 0$. This shows a contradiction, and hence there is no type for $b \not\equiv 0$.

$q = 2$ and H_{q^2} *non-cyclic*. There can be no case in which only one H_p viz. $\{A\}$ is permutable with T_1 or T_2, for if

$$T_1^{-1}BT_1 = C,$$

then

$$T_1^{-1}CT_1 = B,$$

so that $\{BC\}$ is permutable with T. Our relations, accordingly, must be of the form (a). One type is given by the relations

$$T_1^{-1}CT_1 = C^{-1}, \qquad T_1^{-1}BT_1 = B^{-1}, \qquad T_2CT_2 = C, \qquad T_2^{-1}BT_2 = B.$$

This G_{p^34} is the direct product of $\{T_2\}$, $\{A\}$ and $\{T_1, C, B\}$. A second G_{p^34} in which $\{T_2\}$ is not invariant has the relations

$$T_1^{-1}CT_1 = C^{-1}, \qquad T^{-1}BT_1 = B, \qquad T_2CT_2 = C, \qquad T_2^{-1}BT_2 = B^{-1}.$$

23. *$p^2H_{q^2}$ and $p \equiv -1$ mod q.* Here we take $q > 2$, for when $q = 2$ the congruences $p \equiv \pm 1$ (mod q) are identical.

Cyclic H_{q^2}. The H_p whose elements are commutative with T may be taken as $\{A\}$. No other H_p can be permutable with T, for the congruences

$$a^{q^2} \equiv 1 \pmod p \qquad \text{and} \qquad a^q \equiv 1 \pmod p$$

cannot have primitive roots since here $p \not\equiv 1$ (mod q). Since there are $(p^2 + p + 1)H_{p^2}$ in H_{p^3} there is at least one H_{p^2} permutable with T, and evidently this H_{p^2} may be taken as $\{B, C\}$; it cannot be taken as $\{A, B\}$. Evidently we have the following relations:

$$T^{-1}AT = A \qquad T^{-1}BT = C, \qquad T^{-1}CT = B^aC^b.$$

Just as in § 5 we see that $a \equiv -1$, $b \equiv i^p + i$. There are two types accordingly as i (the Galoisian imaginary) is a primitive root of

$$i^{q^2} \equiv 1 \pmod p \text{ or of } i^{q^2} \equiv 1 \pmod p.$$

In the latter case we must have

$$p \equiv -1 \pmod{q^2}.$$

These groups are the direct products of $\{A\}$ and $\{B, C, T\}$.

Non-cyclic H_{q^2}. A is commutative with T_1 and T_2. We may have one type of $G_{p^3q^2}$ with the relations:

$$T_1^{-1}BT_1 = C, \qquad T_1^{-1}CT_1 = B^{-1}C^b \qquad [b = i^p + i],$$
$$T_2^{-1}BT_2 = B, \qquad T_2^{-1}CT_2 = C.$$

This is the direct product of $\{T_2\}$, $\{A\}$ and $\{T_1, B, C\}$. There can be no other type (§ 7).

24. *$p^3H_{q^2}$ and $p \equiv 1$ (mod q).* Let us first take $q > 3$ and H_{q^2} cyclic. Then at least $3H_p$ are permutable with T, since there are $p^2 + p + 1H_p$. Hence we must have the relations:

$$T^{-1}AT = A^a, \qquad T^{-1}BT = B^b, \qquad T^{-1}CT = C^c.$$

We may now have the following cases:

(1)	a, b, c all primitive roots of			$\delta^{q^2} \equiv 1$	(mod p)		
(2)	a, b, c "	"	"	" $\delta^q \equiv 1$	"	"	
(3)	a and b "	"	"	" $\delta^{q^2} \equiv 1$	"	"	
	c	"	"	" $\delta^q \equiv 1$	"	"	
(4)	a	"	"	" $\delta^{q^2} \equiv 1$	"	"	
	b, c	"	"	" $\delta^q \equiv 1$	"	"	

For *case* (1) we may set

$b \equiv a^x$, $c \equiv a^y$ $\pmod p$ $(x, y = lq + k;\ l = 0, 1, 2, \cdots, q-1;\ k = 1, 2, \cdots p-1)$.

Hence our relations above become

$$T^{-1}AT = A^a, \qquad T^{-1}BT = B^{a^x}, \qquad T^{-1}CT = C^{a^y}.$$

To determine the number of types represented by these relations we set

$$T_0 = T^z, \qquad (z = lq + k).$$

We may now get two distinct equivalences by taking z so that

$$\text{(i) } zx \equiv 1, \qquad \text{(ii) } zy \equiv 1 \pmod{q^2}.$$

First. $zx \equiv 1 \bmod q^2$ and $T_0 = T^z$, $A_0 = B$, $B_0 = A$, $C_0 = C$. Therefore $T_0^{-1}A_0T_0 = A_0^a$, $T_0^{-1}B_0T_0 = B_0^{a^z}$, $T_0^{-1}C_0T_0 = C_0^{a^{zy}}$.

Second. $vy \equiv 1 \pmod{q^2}$ and $T_0 = T^v$, $A_0 = C$, $B_0 = B$, $C_0 = A$. Therefore $T_0^{-1}A_0T_0 = A_0^a$, $T_0^{-1}B_0T_0 = B_0^{a^{vx}}$, $T_0^{-1}C_0T_0 = C_0^{a^v}$.

Each pair of values (x, y) furnishes corresponding pairs (z, yz) and (vx, v). Each of these three pairs gives the same type of group. The number of different types is equal to the number of non-corresponding pairs.

Now replace the numbers x, y, z, v by their indices $(\bmod\ q^2)$, that is, we let

$$x \equiv g^{x_0}, \qquad y \equiv g^{y_0}, \qquad z \equiv g^{-x_0}, \qquad v \equiv g^{-y_0} \pmod{q^2}.$$

where g is a primitive root of q^2; and x_0, y_0 take the values $0, 1, 2, 3 \cdots [q(q-1)-1]$. We can now replace our triad of corresponding pairs by (x_0, y_0), $(-x_0, y_0 - x_0)$, $(x_0 - y_0, -y_0)$. Let $l \equiv -y_0$, $m \equiv x_0$, $n \equiv y_0 - x_0$ $[\bmod\ (q^2 - q)]$. The triad of corresponding pairs now becomes

$$(m, -l), \qquad (-m, n), \qquad (-n, l)$$

and we have the congruence

$$l + m + n \equiv 0\ [\bmod\ (q^2 - q)].$$

The number of types depends on the number of solutions of this congruence.

Let x be the number of triads (l, m, n) satisfying the congruence (disregarding order) in which all three constituents of the triad are different, β the similar number in which two only are equal, and γ the similar number in which all three are equal. If

$$q \equiv 1 \pmod 3$$

then

$$q^2 - q \equiv 0 \pmod 3$$

and hence

$$\gamma = 3,$$

for the solutions are

$$l \equiv m \equiv n \equiv 0, \qquad \frac{q^2-q}{3}, \qquad \frac{2(q^2-q)}{3} \quad [\mathrm{mod}\,(q^2-q)].$$

If $$q \equiv 2 \pmod 3$$

then $$q^2 - q \not\equiv 0 \pmod 3$$

and therefore $$\gamma \equiv 1.$$

If two only of the numbers l, m, n are equal, the congruence may be written

$$l + 2m \equiv 0 \quad [\mathrm{mod}\,(q^2-q)].$$

m may have any value except 0, $\frac{1}{3}(q^2-q)$, $\frac{1}{3}[2(q^2-q)]$, and for each value of m there will be one value of l. Therefore if

$$q \equiv 1 \pmod 3$$

then $$\beta = q^2 - q - 3,$$

and if $$q \equiv 2 \pmod 3$$

then $$\beta = q^2 - q - 1.$$

The total number of solutions of all kinds of the congruence, considering the order of the constituents in each triad, is $(q^2-q)^2$ Hence we must have

$$6\alpha + 3\beta + \gamma = (q^2-q)^2.$$

If $q \equiv 1 \pmod 3$ then substituting in the above

$$\alpha = \tfrac{1}{6}(q^4 - 2q^3 - 2q^2 + 3q + 6),$$

and if $q \equiv 1 \pmod 3$ we find that

$$\alpha = \tfrac{1}{6}(q^4 + 2q^3 - 2q^2 + 3q + 2).$$

Let $\alpha_0 =$ the number of solutions α when one constituent of the triad is congruent to 0, and α_1 the number of solutions α when this is not the case. Hence α_0 is the number of solutions of

$$l + m \equiv 0 \; [\mathrm{mod}\,(q^2-q)], \qquad l \not\equiv 0, \qquad m \not\equiv 0,$$

and excluding $l \equiv m \equiv \frac{1}{2}(q^2-q)$. Therefore

$$\alpha_0 = \frac{q^2-q-2}{2}.$$

If $$q \equiv 1 \pmod 3$$

we have $\qquad \alpha_1 = \alpha - \alpha_0 = \frac{1}{6}(q^4 - 2q^3 - 5q^2 + 6q + 12),$

and if $$q \equiv 2 \pmod 3$$

then $\qquad \alpha_1 = \alpha - \alpha_0 = \frac{1}{6}(q^4 - 2q^3 - 5q^2 + 6q + 8).$

The α_1 solutions give α_1 types of groups; while the α_0 solutions give $2\alpha_0$ types of groups, since each triad in this case furnishes two distinct sets of corresponding pairs.

The triads (l, m, m) and $(-l, -m, -m)$ give the same set of corresponding pairs. If $m \equiv \frac{1}{2}(q^2 - q)$ the triads just named form the same solution; but the other triads go in pairs, each pair furnishing one type. Hence from the β solutions mentioned above we get

$$\frac{\beta - 1}{2} + 1 = \frac{\beta + 1}{2} \text{ types.}$$

From γ we get, when $q \equiv 1 \pmod 3$, two types; one corresponding to the triad $(0, 0, 0)$ and a second corresponding to the triad $[\frac{1}{3}(q^2 - q), \frac{1}{3}(q^2 - q), \frac{1}{3}(q^2 - q)]$: while the triad $\{\frac{1}{3}[2(q^2 - q)], \frac{1}{3}[2(q^2 - q)], \frac{1}{3}[2(q^2 - q)]\}$ gives the same type as the second named above. If $q \equiv 2 \pmod 3$ we get a single type corresponding to the triad $(0, 0, 0)$.

In summary, then, for $q \equiv 1 \pmod 3$ the number of types is

$$\tfrac{1}{6}(q^4 - 2q^3 - 5q^2 + 6q + 12) + \frac{q^2 - q - 2}{2} + 2 = \tfrac{1}{6}(q^4 - 2q^3 + 4q^2 - 3q + 6),$$

and for $q \equiv 2 \pmod 3$ the number of types is

$$\tfrac{1}{6}(q^4 - 2q^3 - 5q^2 + 6q + 8) + q^2 - q - 2 + \frac{q^3 - q}{2} + 1 = \tfrac{1}{6}(q^4 + 2q^3 + 4q^2 - 3q + 2).$$

Case (2) in which a, b, c are all primitive roots of $\delta^q \equiv 1 \pmod p$ may be treated in a way similar to the above and the number of types obtained will be exactly the same as is obtained by WESTERN (l. c., p. 237) for $G_{p^3 q}$, viz.:

$$\frac{q^2 + q + 4}{6} \quad \text{if} \quad q \equiv 1 \pmod 3,$$

and $$\frac{q^2 + q}{6} \quad \text{if} \quad q \equiv 2 \pmod 3.$$

Case (3) in which a and b belong to the exponent q^2 and c to the exponent $q \pmod p$ leads to the relations

$$T^{-1}AT = A^a, \qquad T^{-1}BT = B^{a^x}, \qquad T^{-1}CT = C^c.$$

The first two of these relations give $\frac{1}{2}(q^2-q+2)$ types of $G_{p^3q^3}$ (§ 4) and since c may have $q-1$ values, the whole number of types of $G_{p^3q^3}$ is $(q-1)[\frac{1}{2}(q^2-q+2)]$.

Case (4), where a belongs to the exponent q^2 and b, c to the exponent $q(\bmod p)$, gives, in a similar way, $q(q-1)[\frac{1}{2}(q+1)]$ types.

Non-cyclic H_{q^2} $(q>3)$. We may assume the relations

$$(a')\quad \begin{aligned} &T^{-1}AT_1=A^a, && T_1^{-1}BT_1=B^b, && T_1^{-1}CT_1=C^c,\\ &T_2^{-1}AT_2=A^{\alpha}B^{\lambda}c^l, && T_2BT_2=B^{\beta}A^{\mu}C^m, && T_2CT_2=C^{\gamma}A^{\nu}B^n. \end{aligned}$$

We show now that our relations may be so changed that we can assume λ, μ, ν, l, m, $n\equiv 0 \pmod p$. Transformation of A, B, C by T_1T_2 and T_2T_1 shows the relations:

$$\left.\begin{array}{llllll} a\equiv b & \text{or} & \lambda\equiv 0, & a\equiv c & \text{or} & l\equiv 0\\ a\equiv b & \text{or} & \mu\equiv 0, & c\equiv b & \text{or} & m\equiv 0\\ a\equiv c & \text{or} & \nu\equiv 0, & c\equiv b & \text{or} & n\equiv 0 \end{array}\right\} \pmod p.$$

If a, b, c are all congruent $(\bmod p)$ then every H_p is transformed into itself by T_1 and since T_2 transforms $3H_p$ into itself, our relations (a') may be made to take the required form. If a, b, c are not all congruent then two of them, say a and b, are incongruent and hence $\lambda\equiv 0$, $\mu\equiv 0$. We must now consider two cases (i) $a\equiv c$, (ii) $a\not\equiv c$.

In (i) $c\not\equiv b$ and hence $m\equiv 0$, $n\equiv 0$. This gives for the transformation of A and C the relations

$$\begin{aligned} &T^{-1}AT_1=A^a, && T_1^{-1}CT_1=C^c,\\ &T_2^{-1}AT_2=A^{\alpha}C^l, && T_2CT_2=C^{\gamma}A^{\nu}. \end{aligned}$$

Since $a\equiv c$ and $q>2$ we may write our relations

$$\begin{aligned} &T_1^{-1}AT_1=A^a, && T_1^{-1}BT_1=B^b, && T_1^{-1}CT_1=C^c,\\ &T_2^{-1}AT_2=A^{\alpha}, && T_2^{-1}BT_2=B^{\beta}A^{\mu}, && T_2CT_2=C^{\gamma}. \end{aligned}$$

Transformation easily shows that we may assume $\mu\equiv 0$ and hence relations (a') take the required form.

In case (ii) $l\equiv 0$, $\nu\equiv 0$. Here we must consider two subcases:

$$(1)\ c\not\equiv b,\qquad (2)\ c\equiv b.$$

For (1) we see that $n\equiv 0$, $m\equiv 0$ and hence our relations (a') take the required form. The subcase (2) may be easily shown to reduce to the required form

just as in (ii). Hence in every case we may write our relations (a')

$$T_1^{-1}AT_1 = A^a, \qquad T_1^{-1}BT_1 = B^b, \qquad T_1^{-1}CT_1 = C^c,$$
$$T_2^{-1}AT_2 = A^a, \qquad T_2^{-1}BT_2 = B^\beta, \qquad T_2^{-1}CT_2 = C^\gamma.$$

As in the preceding non-cyclic cases we can always make one of the exponents $\alpha, \beta, \gamma \equiv 1 \pmod p$. If all three are congruent to 1 we get

$$\frac{q^2+q+4}{6} \text{ types of } G_{p^3q^2}, \text{ if } q \equiv 1 \pmod 3;$$

and
$$\frac{q^2+q}{6} \text{ types, if } q \equiv 2 \pmod 3.$$

Each of these types is the direct product of $\{T_2\}$ and $\{T_1, A, B, C\}$.

If $\alpha \equiv \beta \equiv 1, \gamma \not\equiv 1$ we get the same number of types as above.

If only one of the exponents α, β, γ belongs to the exponent $q \pmod p$ then there are

$$\left(\frac{q+1}{2}\right)\left(\frac{q^2+q+4}{6}\right) \text{ types for } q \equiv 1 \pmod 3$$

and
$$\left(\frac{q+1}{2}\right)\left(\frac{q^2+q}{6}\right) \text{ types for } q \equiv 2 \pmod 3.$$

We must now consider what happens if $q = 2$ or 3 and there are not three independent H_p permutable with T. If there are three such H_p we may proceed just as above.

$q = 2$; we may assume that only one of the $p^2 + p + 1 H_p$ is permutable with T. Suppose this is $\{A\}$. Therefore $T^{-1}AT = A^a$, $T^{-1}BT = C$. T^2 cannot be commutative with B, for then the group $\{BC\}$ would be transformed into itself, contrary to hypothesis. For the same reason we cannot get a type of G_{4p^3} with our H_{q^2} non-cyclic.

Since T^4 is the lowest power of T commutative with B, any element of H_{p^3} independent of A, we may write

$$T^{-2}BT^2 = T^{-1}CT = A^xB^yC^z.$$

Therefore
$$T^{-3}BT^3 = T^{-2}CT^2 = A^{ax+xz}B^{yz}C^{y+z^2}$$

and
$$B = T^{-4}BT^4 = A^{a^2x+axz+xy+xz^2}B^{y^2+yz^2}C^{2yz+z^3}.$$

Hence we must have the following set of congruences:

$$\left.\begin{aligned} x(a^2+az+y+z^2) &\equiv 0 \\ y(y+z^2) &\equiv 1 \\ z(2y+z^2) &\equiv 0 \end{aligned}\right\} \pmod p.$$

If $z \equiv 0$ then $\{T^2, A, B\}$ is an H_{2p^2} with the $H_{p^2} = \{A, B\}$ invariant, and having $1H_p = \{A\}$ invariant in this H_{2p^2}. Hence there is a second H_p, say $\{B\}$, invariant in this H_{2p^2}. Therefore

$$T^{-2}BT^2 = B^y.$$

Accordingly we may assume $x \equiv 0$ if $z \equiv 0 \pmod p$ and then $y \equiv -1 \pmod p$. We thus get two types of G_{4p^3} according as a belongs to the exponent 2 or exponent 4 (mod p) [cf. § 4 (ii)]. If

$$z \not\equiv 0 \qquad \text{then} \qquad 2y + z^2 \equiv 0.$$

Hence
$$y^2 \equiv -1 \pmod p$$

and accordingly p is of the form $4m + 1$. Therefore

$$p^2 + p + 1 \equiv 3 \pmod 4.$$

Now the $p^2 + pH_p$, aside from $\{A\}$, must be transformed cyclically in sets of $4H_p$ each, for if there were $2H_p$ in any set we should have the case considered above in which $z \equiv 0$. Accordingly we can not get a type of G_{4p^3} with $z \not\equiv 0$.

$q \equiv 3$. Since it is supposed that there are not $3H_p$ permutable with T there are none. Hence

$$T^{-1}AT = B \qquad \text{and} \qquad T^{-1}BT = A^xB^y \text{ or } C.$$

If $T^{-1}BT = A^xB^y$ then $\{A, B, T\}$ is an $H_{p^2q^2}$ having $\{A, B\}$ as an invariant H_{p^2}, and this H_{p^2} has $p + 1$ H_p which are permuted by T, no one of them being invariant.

Hence
$$p \equiv -1 \pmod q.$$

This contradicts the hypothesis that $p \equiv +1 \pmod q$, and accordingly we must assume $T^{-1}BT = C$. If we suppose T^3 commutative with A then we have

$$T^{-1}AT = B, \qquad T^{-1}BT = C, \qquad T^{-1}CT = A,$$

and the group $\{ABC\}$ is invariant under T, contrary to hypothesis.

Evidently the non-cyclic H_{q^2} leads to the same result as above.

Let us suppose T^9 is the lowest power of T commutative with A. The $p^2 + p + 1H_p$ may be transformed in cycles of either $3H_p$ or $9H_p$. If there are $3H_p$ in any one cycle then with

$$T^{-1}AT = B \quad \text{and} \quad T^{-1}BT = C$$

we must have $T^{-1}CT = A^a$, whence

$$T^{-3}AT^3 = A^a, \qquad T^{-3}BT^3 = B^a, \qquad T^{-3}CT^3 = C^a,$$

that is, each of the $p^2 + p + 1H_p$ is transformed into itself by T^3. Since a

cannot be unity it must belong to the exponent 3 (mod p). This furnishes one type of $G_{p^3q^2}$.

If every cycle contains $9H_p$ then we have

$$(\alpha). \qquad p^2+p+1 \equiv 0 \pmod 9$$

Let $\quad p=9k+a; \quad k=0,1,2\cdots; \quad a=1,2,3,\cdots 8.$

Hence $$p^2+p+1 \equiv a^2+a+1 \pmod 9.$$

It is easily seen that $\quad a^2+a+1 \not\equiv 0 \pmod 9$

and hence congruence (α) is impossible, so that we cannot get a type in this case.

25. $\qquad p^3H_{q^2}$ and $p^2+p+1 \equiv 0 \pmod q$.

Cyclic H_{q^2}. Evidently $q \neq 2$, and if $q=3$ the congruences $p\equiv 1$ and $p^2+p+1\equiv 0 \pmod q$ are identical. Hence we need only consider the case in which $q>3$.

None of the H_p can be permutable with T, for $p \not\equiv 1 \pmod q$. The p^2+p+1H_p must fall into sets of q or q^2H_p each, the H_p in each set being permuted cyclically by T. We may assume

$$T^{-1}AT=B \quad\text{and}\quad T^{-1}BT=C$$

for if $$T^{-1}BT=A^xB^y$$

then the $H_{p^2q^2}=\{T, A, B\}$ is a group already treated whose existence depends on the congruence $p\equiv -1 \pmod q$, which is not true here. Hence we must have the relations:

$$T^{-1}AT=B, \qquad T^{-1}BT=C, \qquad T^{-1}CT=A^\alpha B^\beta C^\gamma.$$

We must now consider two cases:

(i) T^q is commutative with C.

(ii) T^{q^2} is the lowest power of T commutative with C.

In case (i) we may proceed just as Western does (loc. cit., pp. 240–4) thus getting a single type of $G_{p^3q^2}$ in which γ, β, α satisfy the relations:

$$\gamma \equiv \lambda+\lambda^p+\lambda^{p^2},$$
$$\beta \equiv -\lambda^{p+1}-\lambda^{p^2+1}-\lambda^{p^2+p},$$
$$\alpha \equiv \lambda^{p^2+p+1} \equiv 1,$$

$\lambda, \lambda^p, \lambda^{p^2}$ being Galoisian imaginaries of the third order and primitive roots of the congruence

$$\lambda^q \equiv 1 \pmod p.$$

Case (ii) also furnishes a single type, the relations being the same as in (i) except that λ, λ^p, p^{p^2} are primitive roots of

$$\lambda^{q^2} \equiv 1 \pmod{p},$$

thus requiring that $\quad p^2 + p + 1 \equiv 0 \pmod{q^2}.$

The procedure in cases (i) and (ii) are so nearly alike that it is unnecessary to go through case (ii).

Non-cyclic H_{q^2}. We may have a single type of $G_{p^3q^2}$ with the relations:

$$T_1^{-1}AT = B, \qquad T_1^{-1}BT_1 = C, \qquad T_1^{-1}CT_1 = A^{\alpha}B^{\beta}C^{\gamma},$$
$$T_2^{-1}AT_2 = A, \qquad T_2^{-1}BT_2 = B, \qquad T_2^{-1}CT_2 = C.$$

This group is the direct product of $\{T_2\}$ and $\{T_1, A, B, C\}$; α, β, γ are determined just as in (i) for the cyclic case.

26. $$H_{p^3} = \{A^4 = 1,\ B^2 = A^2,\ B^{-1}AB = A^3\}.$$

The order of the group of isomorphisms of our H_8 is 24 and since q is a divisor of this order we must have $q = 3$. Evidently there must be $4H_9$. T is commutative with A^2 since $\{A^2\}$ is a characteristic subgroup.

Our H_8 contains three cyclic H_4, viz.:

$$\{A\},\ \{AB\} = \{1, AB, A^2, A^3B\},\ \{B\} = \{1, B, A^2, A^3B\}.$$

Cyclic H_9. T must (1) either be commutative with each of the above H_4 or (2) permute them cyclically. We cannot have the first case, for

$$T^{-1}AT = A^{a}$$

leads to one of the two congruences

$$a^3 \equiv 1 \qquad \text{or} \qquad a^9 \equiv 1 \pmod{4}.$$

and the only value a can have in each case is unity. Hence H_9 is invariant in an H_{36} and, therefore, in the G_{72} contrary to hypothesis.

In the second case we may take

$$T^{-1}AT = B, \qquad T^{-1}BT = AB \qquad \text{or} \qquad A^3B.$$

Hence
$$\begin{aligned} T^{-3}AT^3 &= T^{-1}ABT \qquad \text{or} \qquad T^{-1}A^3BT \\ &= BAB \qquad \text{or} \qquad BAB \\ &= A. \end{aligned}$$

From this we that T^3 is always commutative with A and B. We thus get a single type of G_{72}.

Non-cyclic H_{q^2}. There is a single type with the relations:

$$T_1^{-1}AT_1 = B, \qquad T_1^{-1}BT_1 = AB,$$
$$T_2^{-1}AT_2 = A, \qquad T_2^{-1}BT_2 = B.$$

This G_{72} is the direct product of $\{T_2\}$ and $H_{24} = \{T_1, A, B\}$.

It may be noted that we cannot have a G_{8q^2} with

$$H_8 = \{A^4 = B^2 = 1, B^{-1}AB = A^3\},$$

for here the order of the group of isomorphisms of H_8 is 8 and, therefore, is not divisible by q.

27. $$H_{p^3} = \{A^{p^2} = B^p = 1, B^{-1}AB = A^{p+1}; p \text{ odd}\}.$$

The order of the group of isomorphisms of H_{p^3} is $p^3(p-1)$; and since this must be divisible by q, we have

$$p \equiv 1 \pmod{q}.$$

(i) pH_{q^2}.

Cyclic H_{q^2}. The H_{p^2} with whose elements T is permutable is either $\{A\}$ or $\{A^p, B\}$. In the former case we have

$$T^{-1}AT = A.$$

$\{A^p\}$ is an H_p permutable with T. There are p other H_p, viz.: $\{A^{kp}B\}$, $(k = 0, 1, 2 \cdots p-1)$, forming a conjugate set. On account of the congruence

$$p \equiv 1 \pmod{q}$$

one of these H_p, say $\{B\}$, is permutable with T. Hence

$$T^{-1}BT = B^a.$$

Therefore $$B^{-1}AT = A^{p+1}B^{-1}T = A^{p+1}TB^{-a};$$

also $$B^{-1}AT = B^{-1}TA = TB^{-a}A = TA^{ap+1}B^{-a} = A^{ap+1}TB^{-a}.$$

Hence $$a \equiv 1 \pmod{p}.$$

This makes A, B commutative with T, contrary to hypothesis. The same result follows for *non-cyclic* H_{q^2}. In the latter case we have

$$T^{-1}A^pT = A^p, \qquad T^{-1}BT = B.$$

There are p cyclic H_{p^2} $\{AB^k\}$, $(k = 0, 1, 2, \cdots, p-1)$ and, as in the preceding, one of these, say $\{A\}$, is commutative with T and hence

$$T^{-1}AT = A^a;$$

where a is a primitive root of

$$a^q \quad \text{or} \quad a^{q^2} \equiv 1 \pmod{p^2}.$$

Therefore $$T^{-1}A^pT = A^{ap}.$$

But $$T^{-1}A^pT = A^p,$$

whence $$a \equiv 1 \pmod{p}$$

or $$a = 1 + kp.$$

Therefore $$(1 + kp)^q \quad \text{or} \quad (1 + kp)^{q^2} \equiv 1 \pmod{p^2}$$

which requires that $k \equiv 0 \pmod{p}$, and accordingly A, B, and T are all commutative, contrary to hypothesis. *Non-cyclic* H_{q^2} leads to the same result.

(ii) $p^2H_{q^2}$.

Cyclic H_{q^2}. The H_p with whose elements T is commutative may be taken as $\{B\}$ since it cannot be $\{A^p\}$. One of the p cyclic H_{p^2}, say $\{A\}$, is permutable with T. Hence
$$T^{-1}AT = A^a.$$

This furnishes two types of $G_{p^3q^2}$ according as a belongs to the exponent q or exponent $q^2 \pmod{p^2}$.

Non-cyclic H_{q^2}. We may always assume the relations
$$T_1^{-1}AT_1 = A^a, \qquad T_2^{-1}AT_2 = A^a,$$

for if $$T_2^{-1}AT_2 = (AB^k)^x,$$

then on transforming A with $T_1T_2 = T_2T_1$ we see that either $a \equiv 1$ or $k \equiv 0$. Hence we obtain a single type of $G_{p^3q^2}$ which is the direct product of $\{T_1, A, B\}$ and $\{T_2\}$, since we may assume by a proper change of generators that $a \equiv 1 \pmod{p^2}$.

(iii) $p^3H_{q^2}$.

Cyclic H_{q^2}. One of the p cyclic H_{p^2}, say $\{A\}$, is commutative with T and one of the pH_p, say $\{B\}$, is also commutative with T. Hence
$$T^{-1}AT = A^a, \qquad T^{-1}BT = B^b.$$

Therefore $$T^{-1}B^{-1}ABT = T^{-1}A^{p+1}T = A^{a(p+1)}$$

also $$T^{-1}B^{-1}ABT = B^{-b}T^{-1}ATB^b = B^{-b}A^aB^b = A^{a(bp+1)}.$$

Hence $b \equiv 1 \pmod{p}$ which cannot be true with $p^3H_{q^2}$.

Non-cyclic H_{q^2}. Just as in the cyclic H_{q^2} we may write
$$T_1^{-1}AT = A^a, \qquad T_1^{-1}BT_1 = B$$

and upon transforming A and B with T_2 we may write
$$T_2^{-1}AT_2 = (AB^k)^x, \qquad T_2^{-1}BT_2 = (A^{kp}B)^y.$$

Hence $$T_2^{-1}T_1^{-1}AT_1T_2 = A^{ax-\frac{1}{2}kpax(ax-1)}B^{kax}$$

and $$T_1^{-1}T_2^{-1}AT_2T_1 = A^{ax-\frac{1}{2}kpax(x-1)}B^{kx}.$$

Therefore $$k \equiv 0 \qquad \text{or} \qquad a \equiv 1$$

so that we may assume $$T_2^{-1}AT_2 = A^a.$$

In like manner we may show that

$$T_2^{-1}BT_2 = B^\beta;$$

and just as in the cyclic case above $\beta \equiv 1$; hence we fail to get a type of $G_{p^3q^2}$ with $p^3H_{q^2}$.

28. $H_{p^3} = [A^p = B^p = C^p = 1,\ AB = BA,\ AC = CA,\ C^{-1}BC = AB]$.

(i) pH_{q^2}. We must have $p \equiv 1 \pmod q$.

Cyclic H_{q^2}. As the H_{p^2} whose elements are commutative with T we may take $\{A,\ B\}$. T is permutable with the $p+1H_p$, $\{B\}$ and $\{AB^k\}$, $(k = 0,\ 1,\ 2,\ \cdots p-1)$. Since there are p^2+p+1H_p and since $p^2 \equiv 1 \pmod q$, one of the remaining p^2H_p, say $\{C\}$, must be commutative with T; and so we may write

$$T^{-1}CT = C^a.$$

From $BT = TB$ we get

$$(C^{-1}BC)(C^{-1}TC) = C^{-1}TC)(C^{-1}BC)$$

But $$AB = C^{-1}BC \qquad \text{and} \qquad C^{-1}TC = TC^{-a+1}$$

Hence AB and TC^{-a+1} are commutative. Therefore

$$ABTC^{-a+1} = TC^{-a+1}AB = ATA^{a-1}BC^{-a+1} = A^aBTC^{-a+1}.$$

Hence $$a \equiv 1 \pmod p,$$

which makes C and T commutative, an impossible condition under our hypothesis.

From the above it is evident that there can be no type of $G_{p^3q^2}$ with H_{q^2} *non-cyclic.*

(ii) $p^2H_{q^2}$ and $p \equiv 1 \pmod q$.

Cyclic H_{q^2}. The H_p whose elements are commutative with T may be (1) the invariant characteristic subgroup $\{A\}$ or, (2) some other H_p, say $\{B\}$.

In case (1) $$T^{-1}AT = A.$$

If $q \neq 2$ among the p^2+p remaining H_p, there are at least $2H_p$ commutative with T. Hence

$$T^{-1}BT = B^a, \qquad T^{-1}CT = C^b.$$

From $$C^{-1}BC = AB,$$

we get, since $\quad CT = TC^b \quad$ and $\quad T^{-1}C^{-1} = C^{-b}T^{-1}$,

$$T^{-1}C^{-1}BCT = T^{-1}ABT = AB^a = C^{-b}T^{-1}BTC^b = C^bB^aC^b = A^{ab}B^a.$$

Hence $$ab \equiv 1 \pmod{p}.$$

Accordingly a and b are related and $b = a^{q^2-1}$ or a^{q-1}. We, therefore, get two types of $G_{p^3q^2}$; according as a belongs to the exponents q or exponent $q^2 \pmod{p}$.

Non-cyclic H_{q^2}. As in the case of cyclic H_{q^2} we can assume for one of the non-identical elements of H_{q^2}, say T_1, the following relations

$$T_1^{-1}BT_1 = B^a, \qquad T_1^{-1}CT_1 = C^{a^{q-1}},$$

where a belongs to the exponent $q \pmod{p}$. The most general transformations of B and C by T_2 are

$$T_2^{-1}BT_2 = A^{\alpha}B^{\beta}C^{\gamma}, \qquad T_2^{-1}CT_2 = A^{\lambda}B^{\mu}C^{\nu}.$$

Hence $$T_2^{-1}T_1^{-1}BT_1T_2 = A^{\alpha a - \frac{1}{2}\beta\gamma a(a-1)}B^{\beta a}C^{\gamma a},$$

and $$T_1^{-1}T_2^{-1}BT_2T_1 = A^{\alpha}B^{a\beta}C^{a^{q-1}\gamma}.$$

Since $\quad a \not\equiv 1 \quad$ we have $\quad \gamma \equiv 0, \quad \alpha \equiv 0.$

Similarly by transforming C we find $\lambda \equiv \mu \equiv 0$. Hence we can assume relations as follows:

$$T_1^{-1}BT_1 = B^a, \qquad T_1^{-1}CT_1 = C^{a^{q-1}}, \qquad T_2BT_2 = B^{\alpha}, \qquad T_2^{-1}CT_2 = C^{\alpha^{q-1}}.$$

If $\alpha \not\equiv 1 \pmod{p}$; then, by taking a proper combination of T_1 and T_2 in place of T_2, B can be transformed into itself. Hence we may assume $\alpha \equiv 1 \pmod{p}$. We, therefore, get one type of $G_{p^3q^2}$, the direct product of $\{T_2\}$ and $\{T_1, A, B, C\}$.

If $q = 2$ and two of the $p^2 + pH_p$, besides $\{A\}$, are commutative with T, the above procedure is applicable. Hence we need consider only the case where $q = 2$ and none of the $p^2 + pH_p$ are commutative with T.

The $p^2 + pH_p$, besides $\{A\}$, are transformed by T in cycles of 2 or $4H_p$ each. If any one cycle has $2H_p$ in it then we may assume the relations:

$$T^{-1}AT = A, \qquad T^{-1}BT = C, \qquad T^{-1}CT = B^b.$$

Hence $$T^{-4}BT^4 = B^{b^2} = B.$$

Therefore $$b^2 \equiv \pm 1 \pmod{p}.$$

If $\quad b \equiv +1 \quad$ then $\quad T^{-1}BC^{-1}T = (BC^{-1})^{-1}$

which is contrary to hypothesis. We thus see also that *non-cyclic* H_{q^2} is impossible with $q = 2$. Hence $b \equiv -1$ is the only permissible value. This

furnishes one type of group with the relations:

$$T^{-1}AT = A, \qquad T^{-1}BT = C, \qquad T^{-1}CT = B^{-1}.$$

Next let us suppose that no cycle contains $2H_p$. Consequently every cycle of the $p^2 + pH_p$ contains $4H_p$ and we may write our relations as follows:

$$T^{-1}AT = A, \qquad T^{-1}BT = C, \qquad T^{-1}CT = A^a B^b C^c.$$

Therefore $$T^{-2}BT^2 = T^{-1}CT = A^a B^b C^c$$

and $$T^{-3}BT^3 = T^{-2}CT^2 = A^{a_1} B^{bc} C^{b+c^2},$$

also $$B = T^{-4}BT^4 = T^{-3}CT^3 = A^{a_2} B^{b^2+bc} C^{2bc+c^3}$$

where a_1, a_2 are functions of a, b, c. Hence we must have the congruences:

$$2bc + c^3 \equiv 0 \pmod{p}, \qquad b^2 + bc^2 \equiv 1 \pmod{p}.$$

If $c \equiv 0$, then $b^2 \equiv \pm 1$, a case already considered. Hence we need consider only $c \not\equiv 0$. Therefore

$$2b + c^2 \equiv 0 \pmod{p}, \qquad b^2 \equiv -1 \pmod{p},$$

so that p must be of the form $4n + 1$. Therefore

$$p^2 + p + 1 \equiv 3 \pmod{4}.$$

This means that one cycle must contain $2H_p$, contrary to hypothesis.

We now consider case (2) in which

$$T^{-1}BT = B.$$

If $q \neq 2$, then there are $2H_p$, besides $\{B\}$, permutable with T. Since $\{A\}$ is a characteristic H_p it must be one of our $2H_p$. The other one we may call $\{C\}$.

Hence $$T^{-1}BT = B, \qquad T^{-1}AT = A^a, \qquad T^{-1}CT = C^c.$$

From $C^{-1}BC = AB$ we get on transforming with T

$$T^{-1}C^{-1}BCT = A^a B$$

and since $CT = TC^c$ we have

$$C^{-c}T^{-1}BTC^c = C^{-c}BC^c = A^c B = A^a B.$$

Hence $$c \equiv a \pmod{p}.$$

We thus get two types of $G_{p^3q^2}$, according as a belongs to the exponent q or exponent $q^2 \pmod{p}$.

Non-cyclic H_{q^2}. It is easily seen that we may assume the relations

$$T_1^{-1}BT_1 = B, \qquad T_1^{-1}AT_1 = A^a, \qquad T_1^{-1}CT_1 = C^a,$$
$$T_2BT_2 = B, \qquad T_2AT_2 = A^b, \qquad T_2CT_2 = A^x B^y C^z.$$

By a proper change of generators we can assume $a \equiv 1$; and accordingly $x \equiv y \equiv 0 \pmod p$ so that we get a single type of $G_{p^3q^2}$, the direct product of $\{T_1\}$ and $\{T_2, A, B, C\}$. Just as in the cyclic case we have

$$b \equiv z \pmod p.$$

If $q = 2$, then $1H_p$, $\{B\}$, being permutable with T there are $p^2 + pH_p$ remaining. But $\{A\}$ is also permutable since it is a characteristic H_p. Taking out $\{A\}$ and $\{B\}$ we have left

$$p^2 + p - 1 \equiv 1 \pmod 2.$$

Hence among the $p^2 + p - 1$ H_p one at least, say $\{C\}$, is permutable with T, and hence the case $q = 2$ offers nothing new.

(iii) $p^3H_{q^2}$ and $p \equiv -1 \mod q$.

Here we take $q > 2$ for if $q = 2$ the congruences

$$p \equiv 1 \pmod q \qquad \text{and} \qquad p \equiv -1 \pmod q.$$

are identical.

Cyclic H_{q^2}. Since $\{A\}$ is a characteristic subgroup and $p \equiv -1 \pmod q$, A and T must be commutative. No other H_p can be commutative with T. Hence we have the relations:

$$T^{-1}AT = A, \qquad T^{-1}BT = C, \qquad T^{-1}CT = A^{\alpha}B^{\beta}C^{\gamma}.$$

Proceeding just as Western does (l. c., pp. 251–3), we may show that we get two types of $G_{p^3q^2}$, according as (1) T^q is commutative with C, or (2) T^{q^2} is the lowest power of T commutative with C. In both cases we have

$$\alpha \equiv 0, \qquad \beta \equiv -1, \qquad \gamma \equiv \lambda + \lambda^p \pmod p;$$

where λ is a Galoisian imaginary and a primitive root, in case (1) of $x^q \equiv 1 \pmod p$, and in case (2) of $x^{q^2} \equiv 1 \pmod p$. In the latter case we must have $p \equiv -1 \pmod{q^2}$.

Non-cyclic H_{q^2}. We have one type of $G_{p^3q^2}$ with the relations

$$T_1^{-1}AT_1 = A, \qquad T_1^{-1}BT_1 = C, \qquad T_1^{-1}CT_1 = B^{-1}C^{\gamma},$$

$$T_2AT_2 = A, \qquad T_2^{-1}BT_2 = B, \qquad T_2CT_2 = C,$$

γ having the same value as in case (1) above. This is the direct product of $\{T_2\}$ and $\{T_1, A, B, C\}$.

(iv) $p^3H_{q^2}$. By Sylow's Theorem we have $p^3 \equiv 1 \pmod q$. Since the group of isomorphisms of this H_{p^3} is of order $p^3(p-1)^2(p+1)$ and since q must divide this order we must have $p \equiv 1 \pmod q$.

Cyclic H_{q^2}. If $q > 2$ then at least two of the H_p, besides $\{A\}$, must be permutable with T, so that we have

$$T^{-1}AT = A^a, \qquad T^{-1}BT = B^b, \qquad T^{-1}CT = C^c.$$

Let us transform $C^{-1}BC = AB$ with T. Therefore

$$T^{-1}C^{-1}BCT = T^{-1}ABT$$

and hence
$$A^{bc}B^b = A^aB^b,$$

so that
$$bc = a \pmod p.$$

If a, b, or c belongs to the exponent $q^2 \pmod p$, then the other two do, so that we may put

$$a^x = b \quad \text{and} \quad a^y = c.$$

Therefore
$$x + y \equiv 1 \pmod{q^2}.$$

Neither B nor C can be put in place of A, for A and its powers are the only invariant elements of H_{p^3}. B and C can be interchanged. Accordingly the number of types is the number of solutions of $x + y \equiv 1 \pmod{q^2}$ subject to the condition that $x, y \not\equiv 0, 1$.

If $q = 2$ the congruence has no solutions satisfying our conditions. If $q > 2$ there is one solution

$$x \equiv y \equiv \frac{q^2+1}{2}$$

for which $x \equiv y$, and $\frac{1}{2}(q^2 - 2q - 1)$ for which $x \not\equiv y$. Thus we get

$$\frac{q^2-2q-1}{2} + 1 = \frac{q^2-2q+1}{2}$$

types.

If a belongs to the exponent $q \pmod p$ then b and c do, and the number of types is the number of solutions of

$$x + y \equiv 1 \pmod q,$$

and is, therefore, equal to $\dfrac{q-3}{2} + 1 = \dfrac{q-1}{2}$.

Non-cyclic H_{q^2}. We may assume the relations

$$T_1^{-1}AT = A^a, \qquad T_1^{-1}BT = B^b, \qquad T_1^{-1}CT_1 = C^c,$$
$$T_2^{-1}AT_2 = A^\alpha, \qquad T_2^{-1}BT_2 = B^\beta, \qquad T_2^{-1}CT_2 = C^\gamma.$$

By a proper change of generators we may make

$$\alpha \equiv 1 \quad \text{and then} \quad \beta\gamma \equiv 1 \pmod p.$$

Also just as in the cyclic case $a \equiv bc \pmod p$.

If β and γ belong to the exponent $q \pmod p$ we get $\frac{1}{2}(q-1)$ types of $G_{p^3q^2}$.

If $\beta \equiv \gamma \equiv 1$ we get $\frac{1}{2}(q-1)$ types the direct product of $\{T_2\}$ and $\{T_1, A, B, C\}$.

$q = 2$. Since the case of $3H_p$ commutative with a non-identical element of H_{q^2} is impossible, we need consider only the case in which one H_p is commutative with T or T_1, T_2.

Cyclic H_{q^2}. Since $\{A\}$ is commutative with T we have

$$T^{-1}AT = A^a, \qquad T^{-1}BT = C.$$

T must transform the $p^2 + pH_p$, aside from $\{A\}$, in cycles of $2H_p$ or $4H_p$ each. If any one cycle contains $2H_p$ then we have

$$T^{-2}BT^2 = T^{-1}CT = B^b.$$

We must consider two cases:

$$(1)\ b \equiv +1, \qquad (2)\ b \equiv -1 \pmod p.$$

Now $$T^{-1}C^{-1}BCT = T^{-1}ABT.$$

In case (1) therefore, $$A^{-1}C = A^aC.$$

Hence $$a \equiv -1 \pmod p$$

and $$TA^{\frac{1}{2}(p-1)}BCT = A^{\frac{1}{2}(p-1)}BC,$$

which is contrary to hypothesis.

For case (2) in which $b \equiv -1$ we find from

$$T^{-1}C^{-1}BCT = T^{-1}ABT$$

that $$AC = A^aC.$$

Hence $a \equiv 1$ which is impossible with $p^3H_{q^2}$.

If no cycle contains $2H_p$, then just as in § 28 (ii) we fail to get a type.

Non-cyclic H_{q^2} is evidently impossible.

IV.

$G_{p^3q^2}$ HAVING NEITHER AN INVARIANT H_{q^2} NOR AN INVARIANT H_{p^3}.

The only possible orders for groups of this kind are 72 and 108 (§2).

29. G_{72}. The $4H_9$ have in common an H_3, which is invariant in the G_{72}, thus leading to a factor group Γ_{24}. This Γ_{24} has $3H_8$ or $1H_8$.

(1) If there are $3H_8$ in our Γ_{24}, these H_8 have in common an H_4 which is invariant in the Γ_{24}, corresponding to which we get in G_{72} *an invariant* H_{12}.

(2) If there is $1H_8$ in our Γ_{24}, then there is an invariant H_{24} in our G_{72}; and this H_{24} has $1H_8$ or $3H_8$. If the H_{24} has $1H_8$ it is invariant in the G_{72}, contrary

to hypothesis. If the H_{24} has $3H_8$, then there are only $3H_8$ in our G_{72}; and these $3H_8$ have in common an H_4 invariant in the G_{72}. An invariant H_4 and an invariant H_3 lead to *an invariant* H_{12} of the G_{72}.

Corresponding to the invariant H_{12} obtained in the two cases above, we get a factor group Γ_6 having $1H_3$; and hence G_{72} *has an invariant* H_{36}. This H_{36} must have $4H_9$, for if it had only $1H_9$ this H_9 would be invariant in the G_{72}. The $4H_9$ of the invariant H_{36} have an H_3 (invariant) in common. Hence we get a factor group Γ_{12} with $4H_3$ and, therefore, $1H_4$ which is non-cyclic. Hence H_{36} has an invariant H_{12}. This H_{12} has $1H_4$ or $3H_4$; and these are all the H_4's there are in H_{36}. If there are $3H_4$ in H_{12} and, therefore in H_{36}, these H_4 have an H_2 in common and invariant in H_{36}. We thus get a factor group Γ_{18} having $1H_9$ and, therefore, our invariant H_{36} has an invariant H_{18} containing $1H_9$. Therefore, H_9 is invariant in H_{36} and accordingly in G_{72}, contrary to hypothesis. It follows then that our *invariant* H_{12} *has only* $1H_4$ *which is also invariant in the* H_{36} *and* G_{72}.

The invariant H_4 cannot be cyclic, for then we should have an H_2 invariant in the H_{36}, which was excluded above. In our supposed case, then, we must have an invariant H_4 but not an invariant H_2. The $3H_8$ or $9H_8$ have in common the invariant H_4. The H_8 cannot be of the type

$$A^4 = B^4 = 1\,, \qquad B^2 = A^2\,, \qquad B^{-1}AB = A^3\,,$$

for the invariant H_4 is cyclical.

$9H_8$. The largest subgroup I in which any one of these $9H_8$ is invariant is of order 8. If the $9H_8$ are Abelian, then the invariant H_4 has an H_2 invariant in the G_{72}. Therefore, there is no type of G_{72} with Abelian H_8 in our supposed case.

In our putative case the $9H_8$ must be of the type $A^4 = B^2 = 1\,, B^{-1}AB = A^3$; and we may take as our invariant non-cyclic H_4

$$\{1,\ A^2,\ B,\ A^2B\}.$$

Cyclic H_9. T must transform A^2, B, AB cyclically, while T^3 is permutable with each of them, for $\{T^3\}$ is invariant in G_{72}. Hence we may assume

$$T^{-1}A^2T = B \qquad \text{and} \qquad T^{-1}BT = A^2B.$$

From $A^2T = TB$ we have

(1) $$A^{-2}TA^2 = TBA^2 = TA^2B.$$

Since $\{T,\ A^2,\ B\}$ is our invariant H_{36},

(2) $$A^{-1}TA = T^xA^{2y}B^z.$$

Values of $x,\ y,\ z$ must be so chosen that (1) and (2) harmonize.

T^3 is not permutable with A; for if it were T^3 would be permutable with each element of an H_8, and hence $\{T^3, H_8\}$ = an H_{24} with only $1H_8$, which is impossible. Since $\{T^3\}$ is invariant, $A^{-1}T^3A = T^6$.

With reference to (1) and (2) it is evident that we need to consider only the following values:

$$x = 1,\ 8; \qquad y = 0,\ 1; \qquad z = 0,\ 1;$$

$y = z = 0$ being excluded. This gives six cases to be tested.

(i) $$x = 1, \qquad y = 1, \qquad z = 0.$$

Hence (2) gives $$A^{-1}TA = TA^2,$$

and $$A^{-2}TA^2 = T,$$

not agreeing with (1).

(ii) $$x = 1, \qquad y = 0, \qquad z = 1,$$

$$A^{-1}TA = TB,$$

$$A^{-2}TA^2 = TA^2,$$

again contradictory.

(iii) $$x = 1, \qquad y = 1, \qquad z = 1,$$

$$A^{-1}TA = TA^2B,$$

$$A^{-2}TA^2 = TA^2,$$

again contradictory.

(iv) $$x = 8, \qquad y = 1, \qquad z = 0,$$

$$A^{-1}TA = T^8A^2,$$

$$A^{-2}TA^2 = TA^2B,$$

which agrees with (1).

(v) $$x = 8, \qquad y = 0, \qquad z = 1,$$

$$A^{-1}TA = T^8B,$$

$$A^{-2}TA^2 = T,$$

which contradicts (1).

(vi) $$x = 8, \qquad y = 1, \qquad z = 1,$$

$$A^{-1}TA = T^8A^2B,$$

$$A^{-2}TA^2 = TA^2B,$$

which agrees with (1).

Cases (iv) and (vi) furnish the same type of group; for if in (vi) we replace T by T^2 we get the same relation as in (iv). We thus get a single type of G_{72} defined by the relations

$$A^4 = B^2 = T^9 = 1, \qquad B^{-1}AB = A^3,$$

$$T^{-1}A^2T = B, \qquad T^{-1}BT = A^2B, \qquad A^{-1}TA = T^8A^2.$$

Non-cyclic H_9. As above our H_8 are of the type

$$A^4 = B^2 = 1, \qquad B^{-1}AB = A^3,$$

and our invariant H_4 may be taken as

$$\{1,\ A^2,\ B,\ A^2B\}.$$

Now T_1, T_2 cannot both be permutable with A^2 or B, for then G_{72} would have an invariant H_2, which is not allowable. Hence we may assume

$$T_2^{-1}A^2T_2 = B, \qquad T_2^{-1}BT_2 = A^2B.$$

If $$T_1^{-1}A^2T_1 = B \qquad \text{or} \qquad A^2B,$$

then on transforming A^2 by $T_1T_2^x$ ($x = 2$ in 1st case, 1 in 2nd case) in place of T_1, we find that A^2 and, therefore, also B and A^2B are permutable with $T_1T_2^x$. Hence the elements A^2, B, A^2B may always be taken permutable with T_1.

Since $\{T_1\}$ is our invariant H_3 we must have

$$A^{-1}T_1A = T_1 \quad \text{or} \quad T_1^2.$$

The first case is impossible with $9H_8$ for our G_{72} would be the direct product of $\{T_1\}$ and $\{T_2,\ A,\ B\}$ and accordingly could not contain more than $3H_8$.

Therefore $$A^{-1}T_1A = T_1^2.$$

Since $\{T_1,\ T_2,\ A^2,\ B\}$ is our invariant H_{36}

(3) $$A^{-1}T_2A = T_1^aT_2^xA^{2y}B^z$$

also

(4) $$A^{-2}T_2A^2 = T_2A^2B.$$

Values of a, x, y, z must be so taken as to make (3) and (4) agree. Transformation of (3) by A, when $x = 1$, leads to a contradiction; and if $x = 2$ we find that $a = 0$, $y = z = 1$. Hence

$$A^{-1}T_2A = T_2^2A^2B.$$

Now $\{T_2,\ A,\ B\}$ is an H_{24} with $3H_8$ (cf. Burnside, Theory of Groups p. 104).

Since $$T_1AT_1^{-1} = AT_1$$

we see that there are H_8 not included in the H_{24} above; and hence there must be $9H_8$ in our G_{72}.

We, therefore, have a G_{72} with the defining relations:

$$T_1^3 = T_2^3 = A^4 = B^2 = 1, \qquad B^{-1}AB = A^3, \qquad T_2^{-1}A^2T_2 = B,$$
$$T_2^{-1}BT_2 = A^2B, \qquad A^{-1}T_2A = T_2^2A^2B,$$
$$T_1T_2 = T_2T_1, \qquad A^{-1}T_1A = T_1^2, \qquad B^{-1}T_1B = T_1,$$

$3H_8$. I, the largest subgroup in which an H_8 is invariant, is of order 24. If our H_8 are Abelian no two elements of our invariant H_4 can be conjugate in $I = H_{24}$; for in this H_{24} every element of our invariant H_3 is permutable with every element of an H_8. Hence each element of our invariant H_4 is invariant in G_{72}, giving us an invariant H_2 in G_{72}, which is not allowable.

The only type of H_8 for us to consider is

$$A^4 = B^2 = 1, \qquad B^{-1}AB = A^3.$$

As in the case of $9H_8$ our invariant H_4 may be taken as $\{1, A^2, B, A^2B\}$.

Cyclic H_9. T^3 must be permutable with each element of the above invariant H_4. Since there must not be an invariant H_2 in G_{72} we must have

$$T^{-1}A^2T = B \qquad \text{and} \qquad T^{-1}BT = A^2B.$$

$\{T, A^2, B\}$ is our invariant H_{36}. Hence

(5) $$A^{-1}TA = T^xA^{2y}B^z$$

also

(6) $$A^{-2}TA^2 = TA^2B$$

and

(7) $$A^{-1}T^3A = T^3.$$

Testing the six possible sets of values x, y, z just as in the cyclic H_9 with $9H_8$ we see that no set satisfies the relations (5), (6), (7) and hence no type of G_{72} exists in our supposed case.

Non-cyclic H_9. From the discussion of the non-cyclic H_9 with $9H_8$ it is evident that only a single type of G_{72} is possible under our conditions. The defining relations are

$$T_1^3 = T_2^3 = A^4 = B^2 = 1, \quad B^{-1}AB = A^3, \quad T_2^{-1}A^2T_2 = B, \quad T_2^{-1}BT_2 = A^2B,$$

$$A^{-1}T_2A = T_2^2A^2B, \qquad T_1T_2 = T_2T_1, \qquad B^{-1}T_1B = T_1, \qquad A^{-1}T_1A = T_1.$$

This G_{72} is the direct product of $\{T_1\}$ and $\{T_2, A, B\}$. Since the latter is an H_{24} having $3H_8$ and $4H_3$, our G_{72} must have $3H_8$ and $4H_9$.

We have found above $2H_{36}$ having $4H_9$. This agrees with MILLER, *Quarterly Journal of Pure and Applied Mathematics*, vol. 28, p. 283.

30. G_{108}. The $4H_{27}$ have in common an H_9 invariant in the G_{108}. From the invariant H_9 we get the factor group Γ_{12} with $4H_3$ and, therefore, $1H_4$; corresponding to which in G_{108} we have an invariant H_{36}. Hence there are $3H_4$ or $9H_4$.

If there are $3H_4$ they have in common an H_2 which is invariant in the G_{108}. Corresponding to this invariant H_2, we get a factor group Γ_{54} with $1H_{27}$. Therefore G_{108} has an invariant H_{54} with $1H_{27}$; and hence this H_{27} is invariant

in the G_{108}, contrary to hypothesis. Accordingly the only case we need to consider is $9H_4$.

If our H_{27} are Abelian each element of the invariant H_9 must be invariant in the G_{108}. Hence there could be only $1H_4$ or $3H_4$, both of which cases are excluded under our conditions. It follows, then, that in our supposed G_{108} the H_{27} must be non-Abelian.

Cyclic H_4. The factor group Γ_{12} with $4H_3$ mentioned above is isomorphic with the tetrahedral group; therefore, Γ_{12} has an invariant non-cyclic H_4. From the isomorphism of Γ_{12} and G_{108} we see that the $9H_4$ cannot be cyclic.

Non-cyclic H_4. Suppose the H_{27} are of the type

$$A^9 = B^3 = 1, \qquad B^{-1}AB = A^4.$$

Our invariant H_9 may be taken as $\{A\}$ or $\{A^3, B\}$.

If it is the former then T_1, T_2 cannot both be commutative with A, for then we would not have $9H_4$. Hence one of them, say T_1, must transform A thus:

$$T_1^{-1}AT_1 = A^{-1}.$$

If we also have

$$T_2^{-1}AT_2 = A^{-1},$$

then by keeping T_1 fixed and replacing T_2 by T_1T_2 we see that T_1T_2 transforms A into itself. Hence we may assume

$$T_2^{-1}AT_2 = A.$$

This, however, makes T_2 common to the $9H_4$ and, therefore, invariant in the G_{108}, a case already excluded.

Suppose our invariant $H_9 = \{A^3, B\}$. $2H_3$ of the invariant H_9 are permutable with one of the elements T_1, T_2. Therefore we may write

$$T_1^{-1}A^3T_1 = A^{3\alpha}, \qquad T^{-1}BT_1 = B^{\beta}.$$

We may also write

$$T_2^{-1}A^3T_2 = A^{3a}B^b, \qquad T_2^{-1}BT_2 = A^{3c}B^d.$$

Now

$$T_2^{-1}T_1^{-1}A^3BT_1T_2 = A^{3a\alpha+3c\beta}B^{b\alpha+d\beta}$$

and

$$T_1^{-1}T_2^{-1}A^3BT_2T_1 = A^{3a\alpha+3c\alpha}B^{b\beta+d\beta}.$$

If $\alpha \not\equiv \beta$ then $c \equiv 0$ and $b \equiv 0 \pmod 3$; so that $2H_3$ are invariant under both T_1 and T_2. If $\alpha \equiv \beta$ then all the H_3 in our invariant H_9 are invariant under T_1; and since $2H_3$ are invariant under T_2, we have again $2H_3$ invariant under both T_1 and T_2. Hence we may write our relations as follows:

$$T_1^{-1}A^3T_1 = A^{3\alpha}, \qquad T_1^{-1}BT_1 = B^{\beta},$$

$$T_2^{-1}A^3T_2 = A^{3a}, \qquad T_2^{-1}BT_2 = B^{b}.$$

If α and a are both congruent to 2 (mod 3) then, keeping T_1 fixed and replacing T_2 by T_1T_2, we see that

$$(T_1T_2)^{-1}A^3(T_1T_2) = A^3.$$

Hence we may assume $\alpha \equiv z, a \equiv 1$ unless $a \equiv \alpha \equiv 1$. The latter case is excluded, for then we can make b or $\beta \equiv 1$ so that we have an H_3 invariant in the G_{108}. Hence we may always assume $\alpha \equiv 2, a \equiv 1$.

If $b \equiv 1$, then $\{T_2\}$ is an invariant H_2 of G_{108}, which has been shown impossible in our supposed case. Hence $b \equiv 2$. If now $\beta \equiv 2$ then keeping T_2 fixed and replacing T_1 by T_1T_2 we see that

$$(T_1T_2)^{-1}B(T_1T_2) = B.$$

Hence we can assume $\beta \equiv 1$ and so we have the relations

$$T_1^{-1}A^3T_1 = A^6, \qquad T_1^{-1}BT_1 = B, \qquad T_2^{-1}A^3T_2 = A^3, \qquad T_2^{-1}BT_2 = B^2.$$

Since $\{T_1, T_2, A^3, B\}$ is an invariant H_{36} we have

$$A^{-1}T_1A = T_1^aT_2^bA^{3x}B^y.$$

Let us transform T_1 by $AB = BA^4$.

(i) Let $b = 1$. Hence

$$A^4B^{-1}T_1BA^4 = T_1^aT_2(A^3)^{x+2}B^y,$$

also

$$B^{-1}A^{-1}T_1AB = T_1^aT_2(A^3)^xB^{2+y}.$$

Therefore $x + 2 \equiv x$ and $y + 2 \equiv y$ (mod 3). These congruences being contradictory, it is impossible to get a type in our supposed case with $b = 1$.

(ii) $b = 0$. Hence

$$A^4B^{-1}T_1BA^4 = T_1^a(A^3)^{x+2}B^y,$$

and

$$B^{-1}A^{-1}T_1AB = T_1^a(A^3)^{x+2}B^y.$$

Therefore $x \equiv x + 2$ (mod 3), again contradictory. It follows, then, that we cannot get a G_{108} with the H_{27} taken as above, in our supposed case.

Let us take the H_{27} of the type

$$A^3 = B^3 = C^3 = 1, \qquad AB = BA, \qquad AC = CA, \qquad C^{-1}BC = AB.$$

Without loss of generality we may take our invariant H_9 as $\{A, B\}$. Then our invariant H_{36} is $\{A, B, T_1, T_2\}$. Proceeding just as in the other non-Abelian case it is evident that relations for our invariant H_{36} may be taken as follows:

$$T_1^{-1}AT_1 = A^2, \qquad T^{-1}BT_1 = B, \qquad T_2^{-1}AT_2 = A, \qquad T_2^{-1}BT_2 = B^2.$$

Since $\{T_1, T_2, A, B\}$ is our invariant H_{36}

$$C^{-1}T_1C = T_1^a T_2^b A^x B^y.$$

Let us transform using the fact that $BC = CAB$.

(i) $$b \equiv a \equiv 1.$$

Hence $$C^{-1}B^{-1}T_1BC = T_1T_2A^xB^y,$$

and $$B^{-1}A^{-1}C^{-1}T_1CAB = T_1T_2A^{2+x}B^{2+y},$$

whence $2 \equiv 0 \pmod 3$, an impossible result.

(ii) $$a = 0, \quad b = 1,$$

Hence $$C^{-1}B^{-1}T_1BC = T_2A^xB^y,$$

and $$B^{-1}A^{-1}C^{-1}T_1CAB = T_2A^xB^{2+y}$$

again impossible.

(iii) $$a = 1, \quad b = 0.$$

Hence $$C^{-1}B^{-1}T_1BC = T_1A^xB^y,$$

and $$B^{-1}A^{-1}C^{-1}T_1CAB = T_1A^{2+x}B^y$$

again contradictory.

Evidently we cannot have $a \equiv b \equiv 0$.

There is, then, no G_{108} having neither an invariant H_4 nor an invariant H_{27}.

V.

$G_{p^3q^3}$ HAVING AN INVARIANT H_{p^3} AND ALSO AN INVARIANT H_{q^3}.

32. Since the subgroups H_{p^3} and H_{q^3} have no element in common except 1, we may apply Theorem IX, p. 44, BURNSIDE's *Theory of Groups*, viz.:

If every operation of G transforms H into itself and every operation of H transforms G into itself, and if G and H have no common operation except identity; then every operation of G is permutable with every operation of H.

If $p = 2$, q having any value, there are ten types of $G_{p^3q^3}$ arising from taking the direct product of the five types of H_{p^3} and the two types of H_{q^3}.

Likewise there are ten types of $G_{p^3q^3}$ when p is odd.